ISSN 0178-8930
HZ208361

G 20 141

Zeitschrift für Datenschutz-, Informations- und Kommunikationsrecht

RDV

2/2021

Recht der Datenverarbeitung

Herausgegeben von
Peter Gola · Andreas Jaspers · Rolf Schwartmann · Gregor Thüsing
in Kooperation mit der
Gesellschaft für Datenschutz und Datensicherheit e.V. (GDD), Bonn

Aufsätze

Kurzbeiträge

Rechtsprechung

Aus dem Inhalt

37. Jahrgang
April 2021
Seiten 63–120

GDD
Gesellschaft für Datenschutz und Datensicherheit e.V.

DATAKONTEXT
www.rdv-online.de

Erfüllen Sie Ihre Rechenschaftspflicht!

DATA AGENDA Datenschutz Manager

- ✓ webbasiertes Management System
- ✓ für alle Datenschutzverantwortlichen im Unternehmen und externe Datenschutzbeauftragte
- ✓ einfaches Erfassen und Dokumentieren aller Datenschutzmaßnahmen
- ✓ erleichtert die Zusammenarbeit aller verantwortlichen Stellen
- ✓ expertengeprüft und revisionsicher
- ✓ auch in englischer Sprache verfügbar

Jetzt informieren und 14 Tage kostenlos testen:
www.DataAgenda.de/datenschutzmanager

DATAKONTEXT

Zeitschrift für
Datenschutz–, Informations-
und Kommunikationsrecht

37. Jahrgang 2021
Heft 2
Seiten 63–120

RDV

Recht der Datenverarbeitung

Inhaltsverzeichnis

Beilagenhinweis: GDD-Mitteilungen 2/2021; DATAKONTEXT, Frechen; C.H. Beck, München

Manuskripte:
Zuschriften und Manuskriptsendungen, die den Inhalt der Zeitschrift betreffen, werden an die Schriftleitung erbeten. Für unverlangt eingesandte Manuskripte wird keine Haftung übernommen. Beiträge werden grundsätzlich nur angenommen, wenn sie nicht einer anderen Zeitschrift zur Veröffentlichung angeboten wurden. Mit der Annahme zur Veröffentlichung erwirbt der Verlag vom Autor alle Rechte, insbesondere das Recht der weiteren Vervielfältigung zu gewerblichen Zwecken mit Hilfe fotomechanischer oder anderer Verfahren.

Schriftleitung
Prof. Peter Gola (federführend)
RA Dr. Georg Wronka
RA Andreas Jaspers
RDV-Schriftleitung@gdd.de

Redaktionsanschrift
Birgit Koppitsch
Heinrich-Böll-Ring 10, 53119 Bonn
Telefon: (02 28) 96 96 75-00
Telefax: (02 28) 96 96 75-25
RDV-Redaktion@gdd.de

Erscheinungsweise
6 x jährlich

Bezugspreis

Jahresabonnement	€ 155,–
Einzelheft	€ 25,–

MwSt. im Preis enthalten
jeweils zzgl. Versandkosten

Vertrieb
Dieter Schulz
Tel.: 02234/98949-99
dieter.schulz@datakontext.com

Abo-Service
Telefon: 089-2183-7110
Telefax: 089-2183-32
aboservice@hjr-verlag.de

Abbestellungen
Der Abonnementpreis wird im Voraus in Rechnung gestellt. Das Abonnement verlängert sich zu den jeweils gültigen Bedingungen um ein Jahr, wenn es nicht mit einer Frist von 8 Wochen zum Ende des Bezugszeitraumes gekündigt wird.

Verlag
DATAKONTEXT GmbH, Frechen
Augustinusstraße 9d
D-50226 Frechen-Königsdorf
Telefon: (0 22 34) 9 89 49-30
Telefax: (0 22 34) 9 89 49-32
www.datakontext.com
Geschäftsführung: Dr. Karl Ulrich;
Hans-Günter Böse
HRB 337678

Satz
alka mediengestaltung gmbh
Willmuthstraße 30, 53332 Bornheim-Sechtem

Druck
Grafisches Centrum Cuno GmbH & Co. KG
Gewerbering West 27, 39240 Calbe (Saale)

Anzeigenverwaltung
DATAKONTEXT GmbH, Frechen
Wolfgang Scharf
Telefon: (0 22 34) 9 89 49-60
wolfgang.scharf@datakontext.com
www.datakontext.com

Zeitschrift für
Datenschutz–, Informations- und Kommunikationsrecht
Schriftleitung:
Prof. Peter Gola, Königswinter
(federführend)
RA Dr. Georg Wronka, Bonn
RA Andreas Jaspers, Bonn
Redaktion: Birgit Koppitsch
37. Jahrgang 2021 Heft 2
Seiten 63–120

RDV
Recht der Datenverarbeitung

37. Jahrgang · April 2021 · Seiten 63–120

Editorial

Keine Geschäfte mit Datenschutzverstößen

Datenpannen, unbefugte Bilder im Netz und Fehler in der Datenschutzerklärung auf einer Website als Geschäftsmodell? Diese Tendenz zeichnet sich ab. Wie kann das gehen? Jemand abonniert einen Newsletter auf der Webseite eines Unternehmens, kontaktiert die Firma kurz darauf und verlangt Auskunft über die im Zuge des Abonnements gespeicherten Daten. Dann verlangt er deren Löschung. Im Eifer des Gefechts erteilen Unternehmen in solchen Fällen oft nur unvollständig, falsch oder gar keine Auskunft. Teilweise löschen sie Daten auch vorschnell. In der Folge meldet sich ein Anwalt und verlangt Schadensersatz.[1]

Eine falsche Datenschutzerklärung, eine verspätete Auskunft oder ein Foto im Netz als Schaden? Das ist möglich, weil das Gesetz neben Vermögensschäden auch Ehrschäden für erstattungsfähig erklärt. Die Tendenz, sog. immaterielle Schäden ersetzen zu lassen, ist deutlich erkennbar. 1500 € für die unbefugte Veröffentlichung von Gesundheitsdaten, 500 € pro Monat für die verspätete Erteilung einer nach Datenschutzrecht erforderlichen Auskunft, 300 € für die Veröffentlichung eines Tätigkeitsprofils auf der Website nach dem Ausscheiden eines Arbeitnehmers. Für ein unerlaubtes Foto im Netz kann ein „Schmerzensgeld" bis 1000 € angemessen sein. Das Bundesverfassungsgericht hat kürzlich bestätigt, dass eine einzelne (!) möglicherweise unzulässige Werbemail ein Datenschutzverstoß sein kann. Nun muss der Europäische Gerichtshof entscheiden, ob dafür immaterieller Schadensersatz zu leisten ist.

Datenschutzfehler bei Unternehmen zu provozieren, um sich daran zu bereichern, ist irgendwie mies, aber nicht verboten. Umso sensibler müssen Unternehmen bei der Erfüllung ihrer datenschutzrechtlichen Pflichten sein. Ein Unternehmen kann sich nur dann von Verschulden für den Datenschutzverstoß freisprechen, wenn es nachweisen kann, dass es in keinerlei Hinsicht für die Entstehung des Schadens verantwortlich ist. Das wird selten gelingen. Weil die Gerichte den Ersatzansprüchen teilweise abschreckende Wirkung zusprechen, verschärft sich das Problem.

Wenn dieses Vorgehen Schule macht, dann können Datenschutzverstöße, über die spektakulären Fälle hoher Bußgelder hinaus, flächendeckend zum Problem für die Wirtschaft werden. Der Gesetzgeber kann und sollte hier gegensteuern. Dazu könnte er die Höhe der Anwaltsgebühren für derartige Verfahren so deckeln, dass sie für Anwälte nicht lukrativ sind. So hat man auch das „Abmahnungswesen" bei Urheberrechtsverletzungen in den Griff bekommen.

1 Https://www.gdd.de/downloads/aktuelles/stellungnahmen/21MGInfounredlicheBetroffenenbegehren.pdf

Prof. Dr. Rolf Schwartmann

Prof. Dr. Rolf Schwartmann
Kölner Forschungsstelle für Medienrecht der Technischen Hochschule Köln, Mitherausgeber von Recht der Datenverarbeitung (RDV) sowie Vorsitzender der Gesellschaft für Datenschutz und Datensicherheit e.V. (GDD)

Termine	Thema	Ort	Kontakt
20.04.21	Datenschutz Aktuell	Köln	GDD e.V. und DATAKONTEXT
21.04.21	Planung und Umsetzung der Überwachungsaufgaben des DSB	Köln	GDD e.V. und DATAKONTEXT
22.04.21	IT-Sicherheitsmanagement aus Sicht der DS-GVO	Köln	GDD e.V. und DATAKONTEXT
27.04.21	Konzerndatenschutz	Online-Schulung	GDD e.V. und DATAKONTEXT
27.04.21	Datenschutzverletzungen richtig behandeln	Köln	GDD e.V. und DATAKONTEXT
28.04.21	Hacker-Tools für Datenschutzbeauftragte	Berlin	GDD e.V. und DATAKONTEXT
29.04.21	Strategischer Umgang mit Bußgeldbescheiden bei Datenschutzverstößen	Köln	GDD e.V. und DATAKONTEXT
04.05.21	Datenschutz und Betriebsrat unter der DS-GVO	Online-Schulung	GDD e.V. und DATAKONTEXT
05.05.21	Teleworking unter Beachtung von Datenschutz und Sicherheit	Frankfurt/M.	GDD e.V. und DATAKONTEXT
06.05.21	Verzeichnis von Verarbeitungstätigkeiten	Online-Schulung	GDD e.V. und DATAKONTEXT
06.05.21	Datenschutz-Folgenabschätzung	Frankfurt/M.	GDD e.V. und DATAKONTEXT
10.05.21	Repetitorium GDDcert. EU	Köln	GDD e.V. und DATAKONTEXT
11.05.21	DS-GVO-konforme Verarbeitung personenbezogener Daten mit SAP-Systemen	Berlin	GDD e.V. und DATAKONTEXT
17.05.21	Websites datenschutzkonform gestalten	Online-Schulung	GDD e.V. und DATAKONTEXT
18.05.21	Beschäftigtendatenverarbeitung nach DS-GVO und BDSG	Düsseldorf	GDD e.V. und DATAKONTEXT
18.05.21	Datenschutz-Management light	Online-Schulung	GDD e.V. und DATAKONTEXT
20.05.21	Big Data-Analysen nach DS-GVO und BDSG	Frankfurt/M.	GDD e.V. und DATAKONTEXT
29.05.21	Der neue Kundendatenschutz: Kunden datenschutzkonform gewinnen und binden	Berlin	GDD e.V. und DATAKONTEXT
01.06.21	Datenschutz Aktuell	Online-Schulung	GDD e.V. und DATAKONTEXT
08.06.21	Datenschutz und IT-Sicherheit bei der Nutzung von Clpud Services	Köln	GDD e.V. und DATAKONTEXT
09.06.21	Aktuelle Prüfpraxis der Datenschutzaufsichtsbehörden	Köln	GDD e.V. und DATAKONTEXT
16.06.21	Strafverfolgung, Whistleblowing, Internal Investigations – Datenschutz und Strafrecht	Düsseldorf	GDD e.V. und DATAKONTEXT
17.06.21	Datenschutz-Folgenabschätzung	Online-Schulung	GDD e.V. und DATAKONTEXT
21.06.21	Datenschutzverletzungen richtig behandeln	Online-Schulung	GDD e.V. und DATAKONTEXT
22.06.21	Der neue Kundendatenschutz: Kunden datenschutzkonform gewinnen und binden	Online-Schulung	GDD e.V. und DATAKONTEXT
23.06.21	Zertifizierung zum Betrieblichen Datenschutzbeauftragten (GDDcert. EU)	Köln	GDD e.V. und DATAKONTEXT

Datakontext GmbH, www.datakontext.com, Tel. 0 22 34 / 9 89 49 40

Aufsätze

Prof. Dr. Rolf Schwartmann/Lucia Burkhardt

Proaktiver Bußgeldschutz vor Verwaltungsgerichten im Datenschutzrecht – Rechtssicherheit durch die vorbeugende Feststellungsklage

Spätestens seit den Millionenbußgeldern gegen die 1 & 1 Telekom GmbH und die Deutsche Wohnen schwingt die Angst vor datenschutzrechtlichen Bußgeldern bei so gut wie jeder Datenverarbeitung der Wirtschaft mit, und das durchaus zu Recht. Bußgelder ergingen in der Vergangenheit nämlich nicht nur bei geringer Schuld, sondern auch, und das ist besondere ärgerlich, trotz bestehender Rechtsunsicherheiten (hierzu Abschnitt I). Deren Rechtmäßigkeit ist zwar höchst fraglich, die finanziellen und v.a. rufschädigenden Konsequenzen, die mit einem solchen Bußgeld verbunden sind, stellen dennoch eine erhebliche Gefahr für Unternehmen dar. Aus Unternehmensperspektive bedarf es daher einer Möglichkeit, für Rechtsklarheit zu sorgen, bevor ein Bußgeldbescheid ergeht (hierzu Abschnitt II). Eine solche bietet die vorbeugende Feststellungsklage vor den Verwaltungsgerichten. Deren Voraussetzungen legt der Beitrag dar (hierzu Abschnitt III).

Um einer übereilten und unverhältnismäßigen Verhängung von Bußgeldern zuvorzukommen, kommt unter bestimmten Voraussetzungen vorbeugender Rechtsschutz in Betracht. Hierbei erkennen die Verwaltungsgerichte unter Überwindung der sonst für den Individualrechtsschutz erforderlichen gegenwärtigen Betroffenheit schon in dessen Vorfeld eine Klagemöglichkeit vor dem Verwaltungsgericht an. Konkret kann die Erhebung einer vorbeugenden Feststellungsklage Schutz gewähren. Namentlich die sog. Damokles-Rechtsprechung des Bundesverwaltungsgericht gewährt dem Bürger verwaltungsgerichtlichen Rechtsschutz schon zur Abwehr drohender Bußgelder. So kann mit Blick auf etweige Datenschutzverstöße die Frage geklärt werden, ob ein bestimmtes Verhalten die Vorgaben der DS-GVO erfüllt, und gleichzeitig ein vorschnell verhangenes Bußgeld vermieden werden. Vergleichbare Klagen etwa im Lebensmittel- oder Arzneimittelrecht waren bereits erfolgreich.

I. Die Rechtsunsicherheiten der DS-GVO und das „Damoklesschwert" drohender Bußgelder

Die Datenschutzgrundverordnung entfaltet seit Mai 2018 Wirksamkeit und sorgt seither nicht nur für einen europaweit einheitlichen Schutz personenbezogener Daten, sondern auch für Rechtsunsicherheiten. Denn datenschutzrechtliche Handlungspflichten sind, weil sie Handlungsspielräume zur eigenverantwortlichen Ausfüllung eröffnen, prinzipiell nicht bestimmt formuliert und im hohen Maße auslegungsbedürftig. Sie müssen daher sowohl durch den Rechtsanwender als auch durch Rechtsprechung und Wissenschaft „ausgeformt" und konkretisiert werden. Das verschafft Freiheiten und birgt Risiken. Bei falscher Auslegung droht nämlich die Gefahr einer Sanktionierung per Bußgeld.[1] Diese Bußgelder begründen nicht nur empfindliche finanzielle Risiken für die Verantwortlichen (bis hin zur Gefahr des Existenzverlusts), sie sind häufig auch mit medialer Aufmerksamkeit und daher möglicherweise mit irreversiblen Rufschädigungen verbunden.[2]

Gerade im Bereich des Datenschutzes trägt die Verwaltung in Gestalt der Aufsichtsbehörden besondere Verantwortung und muss mit Bedacht prüfen, ob eine Sanktion nach Art. 58 DS-GVO verhältnismäßig ist. Denn ein Bußgeld sollte stets die Ultima sein. Seine Verhängung verlangt daher eine intensive Begründung, warum eine Untersagung, Anweisung oder eine sonstige Abhilfemaßnahmen nicht genutzt wurde und warum ein Bußgeld in der gewählten Höhe tatsächlich angezeigt ist.[3] Die Praxis zeichnet an vielen Stellen ein anderes Bild.[4] Bußgelder werden nicht nur bei unsicherer Rechtslage, sondern auch bei geringer Schuld, eingeschränktem Risiko für Betroffene und ohne nähere Sachverhaltsermittlung verhängt. Prominentestes Beispiel hierfür ist das Bußgeld des BfDI gegenüber der 1&1 Telecom GmbH in Höhe von fast 10 Millionen Euro wegen eines Verstoßes gegen Art. 25 DS-GVO.[5] Dieses erging, obwohl die

1 LfD Niedersachen Presseerklärung v. 08.01.2021, LfD Niedersachen verhängt Bußgeld über 10,4 Millionen Euro gegen notebooksbilliger.de; BfDI Presseerklärung v. 09.12.2019, BfDI verhängt Geldbußen gegen Telekommunikationsdienstleister.

2 Hierzu ausführlich Schwartmann/Burkhardt, Vorbeugender verwaltungsgerichtlicher Rechtsschutz zur Abwehr drohender Bußgeldverfahren im Datenschutzrecht, bislang nicht veröffentlichtes Gutachten, Teil 1 Abschnitt A sowie Teil 3 Abschnitt B. III. 2. b).

3 Zum Vorrang von Anordnung und Anweisung im Falle bestehender Rechtsunsicherheiten, Schwartmann/Burkhardt, Rechtsschutz (s.o. Fn. 2), Teil 2.

4 Hierzu auch Schwartmann/Burkhardt, Rechtsschutz (s.o. Fn. 2), Teil. 1 Abschnitt A. sowie Teil 3 Abschnitt B. III. 2. b).

5 BfDI Presseerklärung v. 09.12.2019, BfDI verhängt Geldbuße gegen Telekommunikationsdienstleister.

vom Unternehmen implementierten Sicherheitsvorkehrungen der bis dahin gängigen Praxis entsprachen. Dennoch wurden die Verarbeitungsprozesse nicht etwa zunächst beim Betroffenen beanstandet.[6] Ähnlich gelagerte Fälle gibt es viele. Im Januar 2021 wurde bspw. in Niedersachsen ein Bußgeld von 10 Millionen Euro wegen unzulässiger Videoüberwachung ohne vorherige Aufklärung vor Ort verhangen.[7]

Zudem drohen die Aufsichtsbehörden auch dann unspezifisch Bußgelder an, wenn die Rechtslage offen ist. So drohte der Bayerischen LDA im Juni 2020 Geldbußen für eine „Zweckentfremdung der CoronaWarn-App" an.[8] Eine solche sei anzunehmen, sobald Arbeitgeber, Gastwirte oder Ladeninhaber die CoronaWarn-App zum Zwecke der Zugangskontrolle oder des betrieblichen Infektionsschutzes nutzen würden. Das Bayerische LDA sah „keine Gewähr dafür […], dass grundlegende datenschutzrechtliche Anforderungen eingehalten werden können".[9] Gesichert und im Kreis der Aufsichtsbehörden abgestimmt war diese Position zum Zeitpunkt der Presseerklärung nicht. Die Behörde nutzt hier die Zwangssituation, die das „Damoklesschwert" eines drohenden Bußgeldes für potenzielle Adressaten bedeutet, um die eigene Rechtsposition durchzusetzen.

Verantwortliche werden so faktisch gezwungen, den nicht durch verwaltungsbehördliche Ermittlung gedeckten, ungeprüften und möglicherweise fehlerhaften Rechtsansichten der Behörde widerstandslos Folge zu leisten. Die Handlungsspielräume des DS-GVO werden damit de facto auf die Aufsichtspositionen verengt, was im Ergebnis zu massiven Einschränkungen von Art. 12 und 14 GG führt.[10]

II. Prozessuale Konsequenzen

In Fällen, in denen Rechtsunsicherheiten bestehen, namentlich in den oben genannten, wäre der Rückgriff auf mildere Maßnahmen im Rahmen des Art. 58 DS-GVO wie die Anweisung, die Anordnung oder schlimmstenfalls die Untersagung angezeigt, um Rechtssicherheit zu schaffen, bevor sanktionsrechtliche Maßnahmen ergehen. Für eine am Schuldprinzip sowie am Bestimmtheitsgebot orientierte, sprich verfassungskonforme, Sanktionierung wäre dies unbedingt erforderlich.[11]

Ein solches Vorgehen würde den Verantwortlichen zudem die Möglichkeit eröffnen, hinsichtlich strittiger Rechtsfragen ein Gericht anzurufen, ohne Gefahr zu laufen, irreversible wirtschaftliche Schäden zu erleiden. Greifen Behörden jedoch unmittelbar auf Mittel des Ordnungswidrigkeitenrechts zurück, können offene Rechtsfragen nur noch im Rechtsmittelverfahren gegen den Bußgeldbescheid gerichtlich geklärt werden. Im Falle einer Niederlage drohen Verantwortlichen hier aber die genannten finanziellen und rufschädigenden Konsequenzen. Zudem entscheiden die im Datenschutz kaum bewanderten ordentlichen Gerichte.

1. Das Bedürfnis nach vorbeugendem Rechtsschutz

Mit Blick auf diese Gefahren ist es Verantwortlichen kaum zumutbar, einen Bußgeldbescheid regungslos „abzuwarten", der nur droht, weil sie eine andere Rechtsansicht als die Aufsichtsbehörde vertreten. Immerhin kommt der Aufsicht bei der Auslegung der Rechtsbegriffe grundsätzlich keinerlei Beurteilungsspielraum zu.[12] Die Aufgabe, verbindlich über unklare und v.a. strittige Rechtsfragen zu entscheiden, ist alleinige Aufgabe der nationalen Gerichte und des Europäischen Gerichtshofs, nicht der Überwachungsbehörden.[13] Die Behörde unterbreitet im Wege der Anwendung des Rechts lediglich Vorschläge zur Auslegung der unbestimmten Rechtsbegriffe. Daher ist das Vertreten einer nachvollziehbaren aber von der Aufsicht abweichenden Rechtsposition, was die Auslegung der unbestimmten Rechtsbegriffe der DS-GVO angeht, keineswegs unredlich und dürfte insofern kein bußgeldrelevantes Risiko begründen. Für einen hinreichenden Schutz der Verantwortlichen bedarf es daher einer Möglichkeit, für Rechtssicherheit zu sorgen, bevor ein Bußgeldbescheid ergeht, d.h. einer vorbeugenden Klageoption.

2. Die Damokles-Rechtsprechung als Ausweg

Das Ordnungswidrigkeitenrecht kennt eine solche Möglichkeit zwar nicht, Schutz bietet den Verantwortlichen in diesem Fall jedoch der Verwaltungsrechtsweg. Ermöglicht wird dies durch die sogenannte Damokles-Rechtsprechung des Bundesverwaltungsgerichts (BVerwG).[14] Danach kann unter bestimmten Voraussetzungen verwaltungsgerichtlicher Rechtsschutz auch zum Schutz vor Bußgeldern in Anspruch genommen werden. Wenn ein Bußgeld nämlich aufgrund von verwaltungsrechtlichen Zweifelsfragen erging bzw. zu ergehen droht, hat ein potentieller Kläger nach dem BVerwG ein anzuerkennendes Interesse daran, den Verwaltungsrechtsweg als „fachspezifischere" Rechtsschutzform einzuschlagen.[15] Anderenfalls, so betont es auch das BVerwG, hätte es die Behörde im Bereich des Ordnungswidrigkeitenrechts in der Hand, die Bewertung ihrer im Kern verwaltungsrechtlichen Position mittels sofortigen und überscharfen Vorgehens dem Strafrichter zu überantworten.[16]

6 So auch Schwartmann/Burkhardt, Rechtsschutz (s.o. Fn. 2), Teil. 1 Abschnitt A.

7 LfD Niedersachen Presseerklärung v. 08.01.2021, LfD Niedersachen verhängt Bußgeld über 10,4 Millionen Euro gegen notebooksbilliger.de, vgl. auch die Veröffentlichung des Unternehmens v. 08.01.2021, Unverhältnismäßig und unrechtmäßig: notebooksbilliger.de wehrt sich gegen Bußgeldbescheid der Datenschutzbeauftragten, abrufbar unter: https://blog.notebooksbilliger.de/unverhaeltnismaessig-und-unrechtmaessig-notebooksbilliger-de-wehrt-sich-gegen-bussgeldbescheid-der-datenschutzbeauftragten/ (zuletzt abgerufen am: 03.02.2021).

8 Bayerisches LDA Pressemitteilung vom 25.06.2020: Wahrung der Vertraulichkeit bei Kontaktdatenerfassung in der Gastronomie – Keine Zweckentfremdung der Corona-Warn-App.

9 Bayerisches LDA Pressemitteilung vom 25.06.2020: Wahrung der Vertraulichkeit bei Kontaktdatenerfassung in der Gastronomie – Keine Zweckentfremdung der Corona-Warn-App.

10 So auch Schwartmann/Burkhardt, Rechtsschutz (s.o. Fn. 2), Teil. 1 Abschnitt A.

11 HK DS-GVO/BDSG-Schwartmann/Burkhardt, § 41 BDSG (im Anh. zu Art. 83) Rn. 16 ff., 21 ff.

12 BVerfGE 103, 142 (156).

13 Selbst der EDSA, der anders als die Aufsichtsbehörden immerhin über die Befugnis verfügt, die DS-GVO betreffende Fragen zu prüfen und Leitlinien zur Verfügung zu stellen (Art. 70 Abs. 1 S. 2 lit. e), kann über die Auslegung der unbestimmten Rechtsbegriffe nicht verbindlich entscheiden, er erlässt vielmehr sog. Soft Law, vgl. HK DS-GVO/BDSG-Seckelmann Art. 70 Rn. 14.

14 Hierzu ausführlich Schwartmann/Burkhardt, Rechtsschutz (s.o. Fn. 2), Teil. 3 Abschnitt B. III 1.

15 So auch BVerfG, Beschl. vom 07.04.2003 – 1 BvR 2129/02, Rn. 14.

16 BVerwG, Urt. v. 13.01.1969 – I C 86.64, Rn. 19.

III. Die Voraussetzungen der vorbeugenden Feststellungsklage

Statthafte Klageart in den genannten Konstellationen ist die vorbeugende Feststellungsklage[17] gegen die zuständige Aufsichtsbehörde. Mit dieser kann die Frage geklärt werden, ob ein bestimmtes Verhalten die Vorgaben der DS-GVO erfüllt und gleichzeitig ein vorschnell verhangenes Bußgeld vermieden werden. Vergleichbare Klagen etwa im Lebensmittel- oder Arzneimittelrecht waren bereits erfolgreich.

Die Feststellungsklage ergänzt die klassischen Klageoptionen der VwGO (Anfechtungs-, Verpflichtungs- und Leistungsklagen) als eine Art „Auffangklage". Statthaft ist diese nur dann, wenn der Verwaltungsrechtsweg zwar eröffnet ist (hierzu Abschnitt 1), der Kläger seine Rechte jedoch weder mit einer Gestaltungs- noch mit einer Leistungsklage verfolgen kann, sog. Subsidiarität. Besondere Voraussetzungen der Feststellungsklage sind zudem das Vorliegen eines konkreten und streitigen Rechtsverhältnisses (hierzu Abschnitt 2) sowie eines berechtigtes Interesses an der baldigen Feststellung dieses Rechtsverhältnisses (hierzu Abschnitt 3).

1. Eröffnung des Verwaltungsrechtswegs

Da es sich bei der vorbeugenden Feststellungsklage um eine verwaltungsgerichtliche Klage handelt, muss es dem Kläger zunächst um eine verwaltungsrechtliche Streitigkeit gehen.

a) Die Abgrenzung zur Ordnungswidrigkeitensache

Die Klage kann daher zwar erhoben werden, um eine Sanktionierung zu verhindern, nicht aber, um sanktionsrechtliche Fragestellungen zu untersuchen (§§ 63, 67 ff. OWiG).[18] Eine solche wäre bspw. die Frage, wie ein Bußgeld im streitgegenständlichen Fall zu bemessen wäre oder ob Tatbestandsvoraussetzungen wie die Schuld zu bejahen wären. So wird vor den ordentlichen Gerichten gegenwärtig bspw. darüber gestritten, ob juristische Personen selbst schuldhaft handeln können oder ihnen nur Handlungen ihrer Organmitglieder und Repräsentanten zugerechnet werden können.[19]

Zulässig ist die Klage hingegen, wenn sie die verwaltungsrechtlichen Pflichten des Verantwortlichen zum Gegenstand hat, auf die die Tatbestände des Art. 83 Abs. 4-6 DS-GVO Bezug nehmen.[20] In diesem Fall ist trotz des sanktionsrechtlichen Klageziels eine Verwaltungsangelegenheit betroffen. Rechtsfragen hinsichtlich der Auslegung der in der DS-GVO normierten Handlungsgebote haben nämlich grundsätzlich verwaltungsrechtlichen Charakter[21] und zwar auch dann, wenn von der Beantwortung der zu beurteilenden Frage bußgeldrechtliche Bewertungen abhängen. Eine sanktionsrechtliche Relevanz führt nach ausdrücklicher höchstrichterlicher Rechtsprechung nicht dazu, dass eine dem Verwaltungsrecht angehörende Frage ihre diesbezügliche Rechtsnatur verliert.[22]

b) Exkurs: Die Unzumutbarkeit normgerechten Verhaltens als Streitgegenstand

Spätestens seit dem Schrems-II Urteil des EuGH[23] besteht für datenschutzrechtlich Verantwortliche neben den Unsicherheiten, was die konkreten Anforderungen der DS-GVO angeht, ein weiteres Problem. Ungerechtfertigte Sanktionierungen drohen gegenwärtig nämlich nicht nur, weil Rechtsfragen nicht geklärt sind. Die Aufsichtsbehörden drohen seit Schrems-II auch immer wieder Verbote US-amerikanischer Software sowie entsprechende Bußgelder an, obwohl rechtskonformes Verhalten an dieser Stelle schlicht unmöglich erscheint. Da es für eine Datenübermittlung in die USA seit dem Schrems-II Urteil an einer Rechtsgrundlage fehlt, steht der Rechtsverstoß beim Einsatz entsprechender Anwendungen zwar abstrakt fest, ein plötzlicher Verzicht auf US-amerikanische Software erscheint dennoch nur in den wenigsten Fällen machbar. Eine Sanktionierung verstieße daher u.a. wegen fehlender Zumutbarkeit der geforderten Handlung gegen den Verhältnismäßigkeitsgrundsatz.[24]

Auch in dieser Situation ist die Feststellungsklage geeignet, Abhilfe zu schaffen. Zwar handelt es sich bei der Frage nach der Verhältnismäßigkeit einer Sanktionierung typischerweise um einen klassischen Fall der Ausübung des spezifischen Sanktionsermessens. Hat ein Verantwortlicher bspw. ein Bußgeld auferlegt bekommen, weil er in seiner Datenschutzerklärung die Empfänger der von ihm erhobenen Daten nicht hinreichend aufgeschlüsselt hat, ist die Frage nach einer etwaigen Unverhältnismäßigkeit des Bußgeldes mit Blick auf dessen besondere Belastung zu entscheiden (Strafe sollte stets ultima ratio sein).[25] Es handelt sich daher um eine spezifisch sanktionsrechtliche Fragestellung. Ist rechtskonformes Verhalten jedoch unzumutbar oder gar unmöglich, wirkt sich dies nicht nur auf eine potentielle Sanktionierung aus. Die Unverhältnismäßigkeit der Sanktionierung hat keine spezielle sanktionsrechtliche Komponente, sondern beruht auf der Unverhältnismäßigkeit eines entsprechenden verwaltungsrechtlichen Verbotes, sprich auf der Auslegung des Art. 58 Abs. 2 lit. f) bzw. j) DS-GVO i.V.m. § 40 VwVfG. Insofern steht auch in diesem Fall eine verwaltungsrechtliche Fragestellungen zur Entscheidung. Die Fest-

17 Eine Klage konkret gerichtet auf das Unterlassen einer Sanktionierung würde zwar einen Vollstreckungstitel vermitteln und wäre somit rechtschutzintensiver als eine Feststellungsklage. Da in diesem Fall jedoch eine Ordnungswidrigkeitensache betroffen und insofern der Verwaltungsrechtsweg nach § 40 VwGO iVm § § 63, 67 ff. OWiG nicht eröffnet ist (hierzu Abschnitt III. 1.), wäre eine solche Klage indes nicht zulässig.

18 So ausdrücklich auch das BVerwG, Urt. v. 13.01.1969 – I C 86/64, Rn. 18. Vgl. hierzu ausführlich Schwartmann/Burkhardt, Rechtsschutz (s.o. Fn. 2), Teil. 3 Abschnitt B. I. 1.

19 Bejahend kürzlich das LG Bonn, Urt. v. 11.11.2020 – 20 OWi 1/20; abweichend hiervon stellte das LG Berlin, Beschl. v. 18.02.2021 – (526 OWi LG) 212 Js-OWi 1/20 (1/20), 526 OWiG LG 1/20 das Bußgeldverfahren gegen die deutsche Wohnen mangels Benennung der handelnden Person ein.

20 Ausführlich zur Abgrenzung zwischen der Verwaltungs- von der Ordnungswidrigkeitensache Schwartmann/Burkhardt, Rechtsschutz (s.o. Fn. 2), Teil. 3 Abschnitt B. I. 2.

21 So auch Sodan/Ziekow, Sodan, § 43 VwGO, Rn. 85.

22 Vgl. hierzu auch BVerfG, Beschl. v. 07.04.2003 – 1 BvR 2129/02, Rn. 15 welches ausdrücklich klargestellt hat, dass beim Vorliegen unbestimmter Begrifflichkeiten fachgerichtliche Kontrolle in Form des Verwaltungsprozesses, in Abgrenzung zum Strafprozess, in besonderem Maße angezeigt ist.

23 EuGH, Urt. v. 17.07.2020 – C-311/18; so auch Schwartmann/Burkhardt, Rechtsschutz (s.o. Fn. 2), Teil. 3 Abschnitt B. I. 2. a.

24 Dazu eingehend Schwartmann/Burkhardt, Schrems II als Sackgasse für die Datenwirtschaft? Zu den verwaltungsrechtlichen Grenzen datenschutzrechtlicher Nutzungsverbote, ZD 06/2021, 235 ff.

25 HK DS-GVO/BDSG-Schwartmann/Burkhardt, Art. 83 Rn. 27 ff.

stellungsklage ist also geeignet, vor einem Bußgeld zu schützen, welches droht, weil rechtskonformes Verhalten unzumutbar ist.

2. Das Vorliegen eines konkreten und streitigen Rechtsverhältnisses

Da es nicht Aufgabe der Gerichte ist, Rechtsfragen nur um ihrer selbst willen, rechtstheoretisch zu lösen, kann die Feststellungsklage zudem nur zur Klärung eines konkreten Rechtsverhältnisses, d.h. nur unter der Voraussetzung erhoben werden, dass die Anwendung einer Rechtsnorm auf einen bestimmten bereits übersehbaren Sachverhalt streitig ist.[26] Daher bedarf es für die Zulässigkeit der Klage einer irgendwie gearteten Handlung der Aufsichtsbehörde, wodurch diese entweder zum Ausdruck bringt, dass sie meint, ein bestimmtes Tun oder Unterlassen vom Verantwortlichen verlangen zu können, oder aufgrund derer ein solches Vorgehen vom Kläger zu befürchten ist.[27] Das ist etwa dann der Fall, wenn die Behörde versucht die gewünschte Handlung wie im eingangs geschilderten Beispiel mit der Androhung eines Bußgeldes zwangsweise durchzusetzen.

a) Die öffentliche Kommunikation von Rechtspositionen als hinreichende Konkretisierungshandlung

Eine hinreichende „Konkretisierungshandlung", liegt aber auch schon dann vor, wenn eine Behörde die abweichende Würdigung eines Sachverhalts kundtut, ohne eine Vollstreckung dieser Ansicht konkret anzudrohen.[28] Auch ohne ausdrückliche Androhung entsteht beim Verantwortlichen nämlich die begründete Besorgnis, die Behörde könnte ihre Position durchsetzen.[29] Dass die Einleitung von Vollzugsmaßnahmen nicht konkret absehbar ist, hindert die Entstehung eines Rechtsverhältnisses daher nicht, so ausdrücklich das BVerwG.[30]

Ebenso wenig setzt ein streitiges Rechtsverhältnis voraus, dass „zwischen Normadressat und normanwendender Behörde […] Divergenzen offenkundig geworden sein müssten",[31] d.h. auch eine individualisierte Stellungnahme ist nicht unbedingt erforderlich.[32]

Ein der Feststellung zugängliches Rechtsverhältnis entsteht daher schon durch die Kommunikation einer Rechtsauffassung in einer Pressemeldung oder einem Tätigkeitsbericht. Das gleiche gilt, wenn Behördenmitarbeiter Rechtspositionen auf Kanälen wie Twitter publizieren oder diese durch ihre Praxis offenbaren.[33]

b) Stellungnahmen von DSK und EDSA

Genügenden Anlass zur Klage geben zudem auch Stellungnahmen durch DSK und EDSA, obwohl diese selbst über keinerlei Eingriffsbefugnisse gegenüber den datenschutzrechtlich Verantwortlichen verfügen. Denn sowohl DSK als auch EDSA wirken unmittelbar und nachhaltig darauf ein, die konkretisierungsbedürftigen normativen Grundregeln der DS-GVO zu präzisieren, weil ihnen als aller Aufsichtsbehörden übergeordnetes Organ besondere Bedeutung zukommt.[34] Auch wenn ein vollständig einheitlicher Vollzug der Rechtsansichten von DSK und EDSA nicht stets gewährleistet ist bzw. stattfindet, ist die Befolgung der Positionen durch die Aufsichtsbehörden doch aufgrund der angestrebten Harmonisierung und einheitlichen Anwendung der Vorschriften der DS-GVO in der Praxis nicht nur üblich, sondern gerade Sinn der Sache. Die faktische Bindung sollte die Regel sein, weil eine einheitliche Anwendung von der DS-GVO gefordert wird. Nur um sie zu schaffen, tritt die DSK zusammen.[35] Die Positionspapiere von DSK und EDSA entfalten mithin zwar keine Rechtsverbindlichkeit, gleichwohl aber enorme faktische Wirkkraft. Auf die Wiederholung der Position durch die zuständige Aufsichtsbehörde kommt es daher für die Zulässigkeit der Klage nicht mehr an.[36]

3. Die Damokles-Rechtsprechung als Grundlage des Feststellunginteresses

Für die Zulässigkeit einer Feststellungsklage ist über das Vorliegen eines konkreten Rechtsverhältnisses hinaus ein „berechtigtes Interesse an der baldigen Feststellung" der streitgegenständlichen Rechtsfrage erforderlich (§ 43 Abs. 1 VwGO). Hierbei muss es sich nicht um ein rechtliches Interesse handeln, vielmehr genügt jedes schutzwürdige und ausreichend gewichtige Interesse wirtschaftlicher oder aber ideeller Art.[37]

Nach der beschriebenen Damokles-Rechtsprechung ist es dem potenziellen Adressaten eines Bußgeldes nicht zumutbar, „die Klärung verwaltungsrechtlicher Zweifelsfragen auf der Anklagebank erleben zu müssen"[38] (hierzu Abschnitt II. 2.). Deshalb hat der Verantwortliche, droht ihm eine Sank-

26 BVerwG, Urt. v. 08.06.1962 – VII C 78/61; ausführlich hierzu Schwartmann/Burkhardt, Rechtsschutz (s.o. Fn. 2), Teil. 3 Abschnitt B. II. 2 und 3.

27 So auch Sodan/Ziekow-Helge/Sodan, § 43 VwGO Rn. 46; ausführlich hierzu Schwartmann/Burkhardt, Rechtsschutz (s.o. Fn. 2), Teil. 3 Abschnitt B. II. 4.

28 So auch Schoch/Schneider/Bier-Pietzcker, § 43 Rn. 29.

29 Hierzu Schwartmann/Burkhardt, Rechtsschutz (s.o. Fn. 2), Teil. 3 Abschnitt B. II. 4. b).

30 BVerwG, Urt. v. 23.08.2007 – 7 C 13.06, Rn. 32; bezugnehmend hierauf auch VG Köln, Urt. v. 20.04.2018 – 9 K 3859/16, Rn. 46; so auch VG Düsseldorf, Urt. v. 03.09.2002 – 17 K 1907/02, Rn. 49.

31 BVerwG, Urt. v. 23.08.2007 – 7 C 13.06, Rn. 32; bezugnehmend hierauf auch VG Köln, Urt. v. 20.04.2018 – 9 K 3859/16, Rn. 46.

32 Hierzu ausführlich Schwartmann/Burkhardt, Rechtsschutz (s.o. Fn. 2), Teil. 3 Abschnitt B. II. 4. c).

33 Hierzu Schwartmann/Burkhardt, Rechtsschutz (s.o. Fn. 2), Teil. 3 Abschnitt B. II. 4. f) und g).

34 Zur Rolle der genannten Institutionen HK DS-GVO/BDSG-Martini, Art. 68 Rn. 106.

35 So aus Schwartmann/Burkhardt, Rechtsschutz (s.o. Fn. 2), Teil. 3 Abschnitt B. II. 4. d) bb).

36 Hierzu ausführlich Schwartmann/Burkhardt, Rechtsschutz (s.o. Fn. 2), Teil. 3 Abschnitt B. II. 4. d).

37 Sodan/Ziekow-Helge/Sodan, § 43 VwGO Rn. 75; Wysk-Wysk, VwGO § 43 Rn. 51.

38 BVerfG, Beschl. vom 07.04.2003 – 1 BvR 2129/02, Rn. 14; vgl. BVerwG, Urt. v. 09.05.1957 – I C 31.54, Rn. 16; Urt. v. 13.01.1969 – I C 86/64, Rn. 18; Urt. v. 17.01.1972 – 1 C 33.68, Rn. 7; Urt. v. 23.06.2016 – 2 C 18.15, Rn. 20; OVG Münster, Urt. v. 29.01.2014 – 13 A 1901/11, Rn. 25; VGH Baden-Württemberg, Urt. v. 11.02.2010 – 9 S 1130/08, Rn. 16; VG Aachen, Urt. v. 08.12.2017 – 7 K 1859/17; VG Trier, Urt. v. 02.09.2003 – 2 K 471/03. Diese Sichtweise ist auch in der Literatur allgemein anerkannt. Statt aller Posser/Wolff-Möstl, VwGO, § 43 Rn. 19.2; Sodan/Ziekow-Sodan, VwGO, § 43 Rn. 86; Wysk-Wysk, VwGO § 43 Rn. 23, 58. Dieselben Überlegungen liegen auch dem Grundsatz der Subsidiarität der Rechtssatzverfassungsbeschwerde zugrunde, statt aller BVerfG, Urt. v. 14.11.1989 – 1 BvL 14/85, 1 BvR 1276/84.

tionierung aufgrund verwaltungsrechtlicher Zweifelsfragen, ein berechtigtes Interesse daran, um verwaltungsgerichtlichen Rechtsschutz zu ersuchen, d.h. ein berechtigtes Interesse an der feststellenden Beurteilung der strittigen Rechtsfragen.[39]

a) Die Unzumutbarkeit weiteren Abwartens

Es stellt sich indes die Frage, wann ein solches Interesse entsteht. Immerhin setzt die gerichtliche Kontrollfunktion nicht nur im Bereich des Ordnungswidrigkeitenrechts, sondern auch im Verwaltungsprozessrecht grundsätzlich erst nachträglich ein. Für vorbeugenden Rechtschutz bedarf es daher eines sog. qualifizierten Feststellungsinteresses. Dieses Interesse ist v.a. dann gegeben, wenn es dem Betroffenen nicht zuzumuten ist, drohende staatliche Maßnahmen abzuwarten, er insofern unter dem Gebot des effektiven Rechtsschutzes (Art. 19 Abs. 4 GG) nicht auf einen als ausreichend anzusehenden nachträglichen Rechtsschutz verwiesen werden kann.[40] Ein solches Interesse ist die Ausnahme. So ist bspw. das Abwarten etwa einer behördlichen Untersagungsverfügung, die gar nicht unbedingt ergeht, dem Betroffenen angesichts der aufschiebenden Wirkung der Anfechtungsklage (§ 80 Abs. 1 S. 1 VwGO) grundsätzlich zumutbar.[41]

Anders verhält es sich jedoch im Kontext drohender Bußgelder. Sanktionsrechtliche Maßnahmen begründen nämlich vergleichsweise intensive und u.U. irreversible Belastungen. Die durch eine Sanktionsandrohung begründete Zwangslage ist „weitaus größer, als dies bei der Ankündigung eines behördlichen Verbots der Fall ist".[42] Unter dem Damoklesschwert einer drohenden Sanktionierung ist es den Verantwortlichen daher nicht zuzumuten, eine der Behörde zufolge rechtswidrige Praxis, „auf gut Glück" fortzusetzen und Rechtsunsicherheiten bis zur Einleitung eines potenziellen Ordnungswidrigkeitenverfahrens zu erdulden. Schon die besondere Zwangslage eines drohenden Bußgeldes begründet mithin ein Interesse an der „baldigen Feststellung" (§ 43 Abs. 1 VwGO) verwaltungsrechtlicher Zweifelsfragen. Der Erlass eines Bußgeldbescheides ist hierfür nicht erforderlich.[43]

b) Wirtschaftlicher Handlungsdruck als Maßstab

Wie konkret zu befürchten ein Bußgeld hierbei sein muss, damit es „droht"[44] ist bisher gerichtlich nicht entschieden.[45] Die Gerichte[46] haben das Feststellungsinteresse in diesem Kontext bisher regelmäßig auf die ausdrückliche bzw. konkludente Drohung mit einem Bußgeld gestützt. Abgelehnt haben sie ein Feststellungsinteresse dann, wenn die Behörde ausdrücklich klargestellt hatte, dass sie nicht beabsichtige, wegen einer Verletzung der streitgegenständlichen Pflicht gegen den Kläger Straf- oder Bußgeldverfahren einzuleiten,[47] oder aber „hinreichende Anhaltspunkte für ein ordnungswidrigkeitenrechtliches […] Einschreiten nicht mehr gegeben waren".[48] Die Literatur[49] möchte hingegen überwiegend bereits das objektive Verfolgungsrisiko ausreichen lassen, um ein Feststellungsinteresse zu begründen.[50]

Richtigerweise sollte sich die Beurteilung jedoch daran orientieren, worum es bei der Prüfung des qualifizierten Feststellungsinteresse im Kern geht, und damit an der Unzumutbarkeit weiteren Abwartens. Eine solche entsteht jedoch weder allein durch ein objektives Verfolgungsrisiko noch erst mit einer konkreten Sanktionsgefahr. Ein weiteres Ausharren ist vielmehr immer dann unzumutbar, wenn die Sanktionsandrohung wirtschaftlichen Handlungsdruck beim Betroffenen begründet, d.h. einen rational und wirtschaftlich agierenden Verantwortlichen dazu zwingt, auf die Bußgeldgefahr zu reagieren.[51] Stünde dem Adressaten in einer solchen Situation nämlich der Weg über die Feststellungsklage nicht zur Verfügung, wäre er entweder zum Umstellen oder zum Unterlassen der vermeintlich rechtswidrigen Prozesse genötigt, und zwar auch dann, wenn er die Rechtsposition der Behörde nicht teilt. Im Lichte des Gebotes des effektiven Rechtsschutzes darf dem Adressaten also, sobald die Sanktionsandrohung wirtschaftlichen Handlungsdruck auslöst, der Weg über die Feststellungsklage nicht länger verwehrt bleiben.[52]

c) Der wirtschaftliche Zwang zur Reaktion im Datenschutzrecht

Bei der Frage, ob ein vermeintlicher Verstoß gegen die DS-GVO eine Sanktionsgefahr beim entsprechenden Verantwortlichen auslöst, spielt die gegenwärtige Praxis der Datenschutzaufsichtsbehörden eine wichtige Rolle. Die Aufsicht hat nämlich – wie eingangs bereits dargelegt – nicht nur eine Möglichkeit, auf Verstöße zu reagieren, ihr stehen vielmehr neben sanktionsrechtlichen auch verwaltungsrechtliche Abhilfebefugnisse zur Verfügung.[53] Würde die Aufsicht nun bei Verstößen, die im Kern auf bestehenden Rechtsun-

39 Hierzu ausführlich Schwartmann/Burkhardt, Rechtsschutz (s.o. Fn. 2), Teil. 3 Abschnitt B. III. 1. a).

40 BVerwG, Urt. v. 07.05.1987 – 3 C 53/85, Rn. 25 m.w.N.

41 So Lässig, Zulässigkeit der vorbeugenden Feststellungsklage bei drohendem Bußgeldbescheid, NVwZ 1988, 410, 411.

42 BVerwG, Urt. v. 13.01.1969 – I C 86/64.

43 Hierzu auch Schwartmann/Burkhardt, Rechtsschutz (s.o. Fn. 2), Teil. 3 Abschnitt B. III. 1. b).

44 So etwa das VG München, Urt. v. 08.07.2015 – M 18 K 14.1109, Rn. 35.

45 Vgl. Posser/Wolff-Möstl, VwGO, § 43 Rn. 19. Das BVerwG hat bereits 1992 die Frage aufgegriffen, ob nur bei konkreter Androhung von Strafverfahren ein Feststellungsinteresse an der Klärung verwaltungsrechtlicher Fragen bejaht werden kann, vgl. BVerwG, Beschl. v. 26.05.1992 – 3 B 87.91.

46 OVG Münster, Urt. v. 25.08.2017 – 13 B 726/17, Rn. 21; Urt. v. 26.19.2010 – 13 A 929/10; VGH Baden-Württemberg, Urt. v. 11.02.2010 – 9 S 1130/08, Rn. 17.

47 BVerwG, Urt. v. 07.05.1987 – 3 C 53/85, Rn. 25 ff.

48 VGH Baden-Württemberg, Urt. v. 11.02.2010 – 9 S 1130/08, Rn. 17; das BVerwG, Urt. 14.04.2005 – 3 C 31.04, lehnte ein Feststellungsinteresse zudem ab, da „eine drohende Ahndung etwaiger Verstöße […] im vorliegenden Fall gar nicht in Rede" stand; so auch OVG Münster, Urt. v. 25.08.2017 – 13 B 726/17 Rn. 19.

49 Posser/Wolff-Möstl, VwGO § 43 Rn. 19.2; Schoch/Schneider/Bier-Pietzcker, VwGO, § 43 Rn. 20; Sodan/Ziekow-Helge/Sodan, VwGO, § 42 Rn. 50, 89, so auch VG Köln, Urt. v. 20.04.2018 – 9 K 3859/16, Rn. 62; so auch OVG NRW, Beschl. v. 22.06.2017 – 13 B 238/17, Rn. 29; a.A. BVerwG, Urt. v. 14.04.2005 – 3 C 31.04.

50 So aus Schwartmann/Burkhardt, Rechtsschutz (s.o. Fn. 2), Teil. 3 Abschnitt B. III. 2. c).

51 In diese Richtung auch VG Köln, Urt. v. 08.04.2014 – 7 K 3150/12, Rn. 34; VG Düsseldorf, Urt. v. 03.09.2002 – 17 K 1907/02, Rn. 58.

52 Hierzu ausführlich Schwartmann/Burkhardt, Rechtsschutz (s.o. Fn. 2), Teil. 3 Abschnitt B. III. 2. a).

53 Dazu HK DS-GVO/BDSG, Kugelmann/Buchmann, Art. 58 Rn. 39, 111 f.

sicherheiten beruhen, primär auf verwaltungsrechtliche Mittel zurückgreifen, bestünde quasi keine Sanktionsgefahr und damit auch kein Grund auf eine solche wirtschaftlich zu reagieren.

Bußgelder werden in der Praxis aber nicht nur bei geringer Schuld, eingeschränktem Risiko für Betroffene und ohne nähere Prüfung des Sachverhaltsverhängt verhängt, sondern auch bei unsicherer Rechtslage. Der Hamburger Beauftragte für Datenschutz betont ausdrücklich, dass Rechtsunsicherheiten, was Bußgelder anbelangt, nicht zur Passivität der Aufsichtsbehörden, führen könnten.[54] So entsteht, wenn die Handlungspflichten der DS-GVO uneinheitlich ausgelegt werden, eine latente Sanktionsgefahr. Diese begründet, gepaart mit den drakonischen Bußgeldhöhen der DS-GVO, die oft geeignet wären, den Jahresgewinn eines Unternehmens abzuschöpfen,[55] bei den Verantwortlichen unmittelbar das Bedürfnis, auf die Rechtsunsicherheiten zu reagieren.[56] Dies gilt umso mehr, als die Aufsicht den hohen Bußgeldrahmen der DS-GVO in der Vergangenheit auch ausschöpfte und selbst in Fällen bestehender Rechtsunsicherheiten medienwirksame Bußgelder in Millionenhöhe verhängte.[57] Unsicherheiten hinsichtlich der rechtlichen Auslegung der DS-GVO bzw. Uneinigkeiten zwischen Aufsicht und Verantwortlichen hinsichtlich der rechtlichen Bewertung einer Datenschutzpraxis begründen daher stets auch ein qualifiziertes Feststellungsinteresse an deren gerichtlicher Klärung.

IV. Fazit und Ausblick

Die vorbeugende Feststellungsklage vor den Verwaltungsgerichten bietet den Verantwortlichen also Schutz vor vorschneller Sanktionierung, die droht, weil die Aufsicht eine andere Rechtsposition vertritt als der Verantwortliche.

Ein feststellungsfähiges Rechtsverhältnis wird hierbei bereits durch die Veröffentlichung einer von der Datenschutzpraxis des Klägers abweichenden Rechtsansicht begründet. Dies kann sowohl in offiziellen Dokumenten wie Tätigkeitsberichten als auch über Kanäle wie Twitter geschehen. Aufgrund der enormen Bedeutung des EDSA sowie der DSK gilt dies auch für Positionierungen von EDSA und DSK. Im Lichte der teils unvorhersehbaren Bußgeldpraxis einiger Aufsichtsbehörden wird hierdurch zugleich auch unmittelbar das qualifizierte Feststellungsinteresse begründet.

Eine abweichende Beurteilung dürfte sich im Allgemeinen nur dann ergeben, wenn die Aufsichtsbehörden beginnen würden, im Falle unklarer Rechtslagen zunächst auf verwaltungsrechtliche Abhilfebefugnisse zurückzugreifen oder weitere Schritte überhaupt erst ergriffen, wenn Ergebnisse des gegenwärtigen Diskurses zu bestehenden Rechtsfrage absehbar sind, wie es bspw. bei der LDI NRW laut ihres Tätigkeitsberichts 2020 mit Blick auf den Betrieb einer Facebook-Fanpage vor dem Hintergrund der EuGH-Rechtsprechung (Fanpage, Jehova, Fashion ID) der Fall ist.[58]

Derartige Festlegungen bei unsicherer Rechtslage sind wünschenswert. Denn auch dann, wenn Verantwortliche intensiven Gebrauch von der Option der vorbeugenden Feststellungsklage machen würden, bliebe eine Schieflage. Belasten würden die Rechtsunsicherheiten der DS-GVO dennoch vor allem Unternehmen, die bei einer von ihrer Ansicht abweichender Behördenmeinung stets gezwungen wären, vorbeugend tätig zu werden und ein Gericht anzurufen, um existenzielle Risiken zu vermeiden. D.h. Rechtsstreitigkeiten könnten nicht erst dann gerichtlich ausgetragen werden, wenn es im Verlauf eines Verwaltungsverfahrens tatsächlich zu Meinungsverschiedenheit zwischen einem Verantwortlichen und der Aufsicht käme, die auch die einem Verwaltungsprozess immanente Anhörung nicht aus der Welt schaffen konnte. Ebenso wenig müsste die Behörde so im Einzelfall ermitteln oder aber einen schriftlichen und begründeten Bescheid erlassen, auf welchen sich etwaiige Klagen konkret beziehen könnten. Ob dies tatsächlich so gewollt ist, ist höchst fraglich.

Prof. Dr. Rolf Schwartmann
Kölner Forschungsstelle für Medienrecht der Technischen Hochschule Köln, Mitherausgeber von Recht der Datenverarbeitung (RDV) sowie Vorsitzender der Gesellschaft für Datenschutz und Datensicherheit e.V. (GDD)

Lucia Burkhardt
Wissenschaftliche Mitarbeiterin an der Kölner Forschungsstelle für Medienrecht an der Technischen Hochschule Köln.
Foto: TH Köln/Schmülgen

54 HmbBfDI Tätigkeitsbericht Datenschutz 2019, S. 106.

55 So HK DS-GVO/BDSG-Schwartmann/Jacquemain, Art. 83 Rn. 11, 135.

56 Ausführlich hierzu Schwartmann/Burkhardt, Rechtsschutz (s.o. Fn. 2), Teil. 3 Abschnitt B. III. 2. b).

57 So auch Schwartmann/Burkhardt, Rechtsschutz (s.o. Fn. 2), Teil. 3 Abschnitt B. III. 2. b) bb).

58 LDI NRW Tätigkeitsbericht 2020, S. 21 f.

Prof. Dr. Boris P. Paal, M. Jur. (Oxford)

Bußgeldzumessung im Datenschutzrecht

Aktuelle Fragestellungen und Problemkreise (zugleich Besprechung von LG Bonn, Urteil vom 11.11.2020 – 29 OWi 1/20 = RDV 2021, 48)

Die Datenschutz-Grundverordnung (im Folgenden: DS-GVO) hat auch und gerade infolge des im Vergleich zur vormaligen Rechtslage deutlich erhöhten Bußgeldrahmens an Praxisrelevanz gewonnen. Auf die veränderten rechtlichen Rahmenbedingungen haben die deutschen Datenschutzbehörden reagiert und ihre Sanktionspraxis angepasst. So ergingen in den vergangenen Monaten hohe datenschutzrechtliche Bußgelder unter anderem gegen den Modekonzern H&M in Höhe von € 35,3 Mio.,[1] gegen die Immobiliengesellschaft Deutsche Wohnen SE in Höhe von € 14,5 Mio.[2] und gegen den Telekommunikationsdienstleister 1&1 Telecom GmbH in Höhe von € 9,55 Mio.[3] Im letztgenannten Fall liegt nun erstmals ein Gerichtsurteil[4] zur aktualisierten Bußgeldpraxis der deutschen Datenschutzbehörden vor. Mit Beschluss vom 18.02.2021 hat zudem unlängst das LG Berlin im Bußgeldverfahren gegen die Deutsche Wohnen SE entschieden.

I. Urteil des LG Bonn

Die 9. Kammer für Bußgeldsachen des Landgerichts (im Folgenden: LG) Bonn stimmt in ihrem Urteil vom 11.11.2020 (Az. 29 OWi 1/20) zwar in vielen Punkten überein mit der Beurteilung des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit (im Folgenden: BfDI), der im Dezember 2019 das Bußgeld gegen die 1&1 Telecom GmbH erlassen hatte. In einem zentralen Aspekt weicht das Urteil aber wesentlich von dem Bußgeldbescheid ab: Es wird der Betrag der verhängten Geldbuße drastisch reduziert, wobei sich das Gericht auch mit dem neuen Bußgeldkonzept[5] der deutschen Datenschutzkonferenz (im Folgenden: DSK), eines Zusammenschlusses der Datenschutzbehörden des Bundes und der Länder, aus dem Jahr 2019 auseinandersetzt.

1. Zugrundeliegender Sachverhalt

Anlass für die Verhängung des Bußgelds gaben die nach Auffassung des BfDI unzureichenden Anforderungen an die Authentifizierung der Kunden des Telekommunikationsdienstleisters 1&1 bei der Nutzung einer Telefon-Hotline. So konnten Unberechtigte bereits durch die Angabe von Namen und Geburtsdatum einer Person weitreichende Informationen zu deren Vertrag mit 1&1 erhalten.

Zwar wurde im Fall eines Anrufs bei dem Callcenter der 1&1 Telecom GmbH auf erster Stufe im Rahmen einer Identifizierung des Kunden danach unterschieden, ob der Anruf von einer Telefonnummer getätigt wurde, die der Telekommunikationsdienstleister selbst vergeben hatte oder ob es sich um eine „externe" Telefonnummer handelte. Zur anschließenden Authentifizierung genügte aber bereits die Angabe des Geburtsdatums des Kunden auch dann, wenn es sich bei dem Anrufer erkennbar nicht um den Kunden selbst, sondern um einen Dritten handelte. Für diese – dem Urteil des LG Bonn zugrundeliegende – Konstellation existierten insoweit keine weiteren sichernden Vorgaben. Vielmehr wurden für den Kunden handelnde, diesem nahestehende Personen im Regelfall auch ohne ausdrückliche Legitimation durch den Kunden als (vertretungs-)berechtigt angesehen. In Anbetracht dessen bestand ein substantielles Risiko für die Rechte und Freiheiten der Kunden der 1&1 Telecom GmbH, das sich insbesondere in einer unerwünschten Kontaktaufnahme bis hin zum „Stalking" manifestieren konnte und aus dem materielle wie immaterielle Schäden zu erwachsen drohten.

Im konkret gerügten Fall ging es um die ehemalige Lebensgefährtin eines Kunden, die durch einen Anruf bei der Hotline unter anderem dessen neue Rufnummer erhalten hatte. Nach alledem sah der BfDI einen Verstoß gegen die Pflicht zur Implementierung hinreichender technischer und organisatorischer Maßnahmen aus Art. 32 Abs. 1 DS-GVO als gegeben an und verhängte daher ein Bußgeld in Höhe von € 9,55 Mio. gegen die 1&1 Telecom GmbH.[6] Gegen diesen Bußgeldbescheid wandte sich das Unternehmen vor dem LG Bonn. In Ermangelung eines hinreichend sicheren Authentifizierungsverfahrens hat das Gericht das Vorliegen eines Datenschutzverstoßes seitens des Unternehmens – in Übereinstimmung mit dem BfDI – bejaht: Es wird festgehalten, dass die 1&1 Telecom GmbH gegen Art. 83 Abs. 4 Buchst. a) i.V.m. Art. 32 Abs. 1 DS-GVO verstoßen habe, da es jedenfalls grob fahrlässig unterlassen worden sei, Prozesse zur hinreichenden Authentifizierung von Anrufern zu gewährleisten.[7] Den als Sanktion für diesen Verstoß festgesetzten Betrag hat das Gericht aber im Ergebnis als unangemessen hoch angesehen.

2. Gegenstand und Ziele des Beitrags

Vor dem Hintergrund der aktualisierten Bußgeldpraxis der deutschen Aufsichtsbehörden, die auf dem neuen Berech-

1 Hamburgischer Beauftragter für Datenschutz und Informationsfreiheit, PM vom 01.10.2020, abrufbar unter https://datenschutz-hamburg.de/pressemitteilungen/2020/10/2020-10-01-h-m-verfahren (zuletzt abgerufen am 25.02.2021).

2 Berliner Beauftragte für Datenschutz und Informationsfreiheit, PM vom 05.11.2019, abrufbar unter https://www.datenschutz-berlin.de/fileadmin/user_upload/pdf/pressemitteilungen/2019/20191105-PM-Bussgeld_DW.pdf (zuletzt abgerufen am 25.02.2021).

3 Bundesbeauftragter für Datenschutz und Informationsfreiheit, PM vom 09.12.2019, abrufbar unter https://www.bfdi.bund.de/DE/Infothek/Pressemitteilungen/2019/30_BfDIverh%C3%A4ngtGeldbu%C3%9Fe1u1.html (zuletzt abgerufen am 25.02.2021).

4 LG Bonn, Urt. v. 11.11.2020 – 29 OWi 1/20 = RDV 2021, 48.

5 DSK, Konzept der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder zur Bußgeldzumessung in Verfahren gegen Unternehmen, 14.10.2019.

6 Bundesbeauftragter für Datenschutz und Informationsfreiheit, PM vom 09.12.2019, abrufbar unter https://www.bfdi.bund.de/DE/Infothek/Pressemitteilungen/2019/30_BfDIverh%C3%A4ngtGeldbu%C3%9Fe1u1.html (zuletzt abgerufen am 25.02.2021).

7 LG Bonn, Urt. v. 11.11.2020 – 29 OWi 1/20 = RDV 2021, 48, Rn. 63 ff.

nungsmodell der DSK basiert, der allgemeinen Kritik am DSK-Konzept und der besonderen Problemlagen im Fall der 1&1 Telecom GmbH ist das Urteil des LG Bonn mit Spannung erwartet worden. Zunächst wirft die erstmalige Auseinandersetzung eines Gerichts mit einem nach dem neuen DSK-Konzept verhängten Bußgeld die Frage auf, welche Position das LG Bonn zu dem Bußgeldkonzept einnimmt. Zudem waren durch das Gericht grundsätzliche dogmatische Fragen zur DS-GVO und zu deren Zusammenspiel mit dem nationalen (Bußgeld-)Recht – so insbesondere betreffend die Erforderlichkeit des Vorliegens eines Verstoßes einer Leitungsperson und das Schuldprinzip – zu behandeln. Der vorliegende Beitrag befasst sich mit den hierdurch aufgeworfenen datenschutzrechtlichen Problemkreisen im Kontext der Bußgeldzumessung nach der DS-GVO, bezieht hierzu Stellung und geht auf Praxisfolgen ein.

II. Verbandshaftung/Handlungszurechnung

Nach vorangegangener Feststellung des Vorliegens eines Datenschutzverstoßes lässt das LG Bonn für die Sanktionierung der 1&1 Telecom GmbH genügen, dass dieser Verstoß seitens irgendeines Mitarbeiters des Unternehmens begangen wurde.[8] Das Gericht lehnt die Anwendung der nationalen Zurechnungsvorschrift des § 30 OWiG ab und hält somit die Feststellung des Verstoßes einer natürlichen (Leitungs-)Person des Unternehmens gegen die datenschutzrechtlichen Bestimmungen für nicht erforderlich.[9] Damit positioniert sich das Gericht bereits in diesem Kontext jedenfalls mittelbar zu der kontrovers diskutierten Frage betreffend die Verwendung eines sogenannten „funktionalen Unternehmensbegriffs" nach unionskartellrechtlichem Vorbild im Datenschutzbußgeldrecht, als deren Konsequenz sich eine unmittelbare Verbandshaftung ergibt.[10]

1. Anwendbarkeit des mitgliedstaatlichen Sanktionenrechts

Das deutsche Recht geht hinsichtlich der Haftung von Unternehmen für Straftaten oder Ordnungswidrigkeiten vom sogenannten Rechtsträgerprinzip aus. Danach ist eine direkte Sanktionierung juristischer Personen oder Personenvereinigungen nur über die Zurechnungsvorschrift des § 30 OWiG für den Fall möglich, dass eine im Katalog des § 30 Abs. 1 OWiG genannte natürliche Leitungsperson die jeweilige Straftat oder Ordnungswidrigkeit begangen hat. Ganz grundlegend stellt sich insoweit die Frage – mit der sich letztlich auch das LG Bonn beschäftigt –, ob und inwieweit (materielle) mitgliedstaatliche Vorschriften im Wege einer „Lückenschließung" hier überhaupt herangezogen werden können. Die Anwendbarkeit des § 30 OWiG im Rahmen von nach Art. 83 Abs. 4 bis 6 DS-GVO zu sanktionierenden Datenschutzverstößen legt der umfassende Verweis des § 41 Abs. 1 S. 1 DS-GVO auf das OWiG – und auch der Umstand, dass § 41 Abs. 1 S. 2 DS-GVO keine entsprechende Ausnahme von der Verweisung vorsieht – nahe.[11] Die Verordnung selbst trifft hingegen keine (ausdrückliche) Festlegung hinsichtlich einer § 30 OWiG vergleichbaren Zurechnung von Datenschutzverstößen.

Eines der zentralen Ziele der DS-GVO ist – auch und gerade mit Blick auf die vorherige Rechtslage unter Geltung der Datenschutz-Richtlinie (im Folgenden: DS-RL) – die Vereinheitlichung der Befugnisse und Sanktionen innerhalb der Mitgliedstaaten.[12] Der Erreichung dieses Ziels wäre es abträglich, wenn die Mitgliedstaaten letztlich weiterhin ihre nationalen Vorschriften zur Anwendung bringen könnten. So steht auch der in Art. 4 Abs. 3 EUV verankerte unionsrechtliche Effektivitätsgrundsatz (effet utile) einer Schwächung der Durchsetzung unionsrechtlicher Regelungen durch die Anwendung nationaler Regelungen entgegen.

2. Unmittelbare Verbandshaftung

Vor diesem Hintergrund fordert Erwägungsgrund 150 S. 3 DS-GVO die Anknüpfung an den unionskartellrechtlichen Unternehmensbegriff bei der Verhängung von Geldbußen gegenüber Unternehmen. Hiernach soll der Begriff „Unternehmen" im Sinne der Art. 101, 102 AEUV und damit unionskartellrechtlich verstanden werden. Neben weiteren Implikationen[13] ist eine Konsequenz der Verwendung dieses „funktionalen Unternehmensbegriffs"[14] die unmittelbare Verbandshaftung im Sinne eines Funktionsträgerprinzips. In diesem Sinne haftet das Unternehmen als funktionale Einheit unmittelbar für den Verstoß (irgend-)eines Mitarbeiters, der nicht einmal bestimmbar sein muss.[15] Der einzelne Rechtsträger bleibt zwar formal betrachtet Adressat des Bußgeldbescheides.[16] In die Haftung genommen wird aber (gesamtschuldnerisch) letztlich der gesamte Konzern.[17]

3. Ausführungen des LG Bonn

Die beschriebene Problematik greift zu Recht auch das LG Bonn auf. Das Gericht führt in diesem Kontext aus, die uneingeschränkte Anwendbarkeit mitgliedstaatlicher Regelungen habe nicht nur eine uneinheitliche Sanktionspraxis innerhalb der Union zur Folge, sondern betreffe auch die Effektivität der Durchsetzung.[18] Konkret würde dies in Bezug auf die Anwendbarkeit der nationalen Vorschrift des § 30 OWiG bedeuten, dass eine umfangreiche Sachverhaltsaufklärung erforderlich wäre, um den intern für den Datenschutzverstoß Verantwortlichen zu ermitteln. Nach zutreffender Auffassung des Gerichts würde dies zu einer „erheblichen Einschränkung der Bußgeldverhängung gegen Unternehmen

8 LG Bonn, Urt. v. 11.11.2020 – 29 OWi 1/20 = RDV 2021, 48, Rn. 43.

9 LG Bonn, Urt. v. 11.11.2020 – 29 OWi 1/20 = RDV 2021, 48, Rn. 51 ff.

10 Zum Streitstand um den funktionalen Unternehmensbegriff siehe nachfolgend Abschnitt IV.3.

11 So Gola/Gola, Datenschutz-Grundverordnung, 2. Aufl. 2018, Art. 83 DS-GVO Rn. 11.

12 Vgl. etwa die Erwägungsgründe 9, 11, 13 DS-GVO.

13 Weitere Konsequenzen sind die Konzernhaftung und die Zugrundelegung des Konzernumsatzes im Rahmen der Bußgeldzumessung. Grundsätzlich zur Bußgeldzumessung siehe zudem nachfolgend Abschnitt IV.

14 Loewenheim/Meessen/Riesenkampf/Kersting/Meyer-Lindemann/Grave/Nyberg, Kartellrecht, 4. Aufl. 2020, Art. 101 AEUV Rn. 97 ff.

15 Vgl. Karlsruher Kommentar/Rogall, Ordnungswidrigkeitengesetz, 5. Aufl. 2018, § 30 OWiG Rn. 279.

16 Dazu Kokott/Dittert, WuW 2012, 670, 671 m.w.N.

17 Hierzu Loewenheim/Meessen/Riesenkampf/Kersting/Meyer-Lindemann/Grave/Nyberg, Kartellrecht, 4. Aufl. 2020, Art. 101 AEUV Rn. 178 ff.

18 LG Bonn, Urt. v. 11.11.2020 – 29 OWi 1/20 = RDV 2021, 48, Rn. 53.

führen".[19] Bekräftigt wird dieses Argument durch den Befund, dass Art. 83 Abs. 8 DS-GVO eine Öffnung für mitgliedsstaatliche Regelungen lediglich hinsichtlich verfahrensrechtlicher Vorschriften vorsehe, während § 30 OWiG einen darüber hinausgehenden Regelungsgehalt aufweise.[20] Nach Auffassung des LG Bonn verbietet sich also im Ergebnis ein Abstellen auf nationale Zurechnungsregelungen. Das Gericht fordert damit keine nähere Bestimmung des für den datenschutzrechtlichen Verstoß verantwortlichen Mitarbeiters. Vielmehr wird es als ausreichend erachtet, dass im Bußgeldbescheid lediglich der Verstoß näher dargestellt wird.

4. Stellungnahme / Rechtsvergleichende Perspektive

Obwohl die Übertragung des funktionalen Unternehmensbegriffs auf das Datenschutzbußgeldrecht als solche durchaus kritisch zu hinterfragen ist,[21] ist das von dem LG Bonn gefundene Ergebnis hinsichtlich der Nichtanwendung des § 30 OWiG und die damit zusammenhängende Ablehnung des Erfordernisses eines Verstoßes durch eine Leitungsperson somit insgesamt als folgerichtig zu bewerten.[22] Die Handlungszurechnung erfolgt einzig auf der Grundlage und am Maßstab des Unionsrechts.

Die Brisanz dieser Zurechnungsfragen zeigt sich auch anhand eines Vergleichs mit der jüngeren Sanktionierungspraxis und der hierzu ergangenen Judikatur in Österreich. In einem vergleichbaren Fall, der dem Bundesverwaltungsgericht der Republik Österreich vorlag, hatte das Gericht die § 30 OWiG entsprechende Zurechnungsvorschrift, i.e. § 30 öDSG, für weiterhin anwendbar befunden und den Anwendungsvorrang der Art. 83 Abs. 4 bis 6 DS-GVO verneint.[23] Während in Deutschland eine Sanktionierung stattfinden könnte, ohne dass der verantwortliche Mitarbeiter zu ermitteln und zu benennen sein muss, soll auf dieser Grundlage in Österreich kein Bußgeld verhängt werden können. Kann also der Mitarbeiter des österreichischen Unternehmens, durch den der Datenschutzverstoß begangenen worden war, nicht (mehr) identifiziert werden, entfiele eine Sanktionierung des Unternehmens gänzlich. Eine solch uneinheitliche Rechtspraxis innerhalb der Mitgliedstaaten dürfte nicht als vom Verordnungsgeber intendiert angesehen werden können.

III. Verschulden des Verantwortlichen

Das LG Bonn streift weiter die Frage nach dem Bestehen eines Verschuldenserfordernisses im Rahmen des Datenschutzverstoßes. Eine verschuldensunabhängige Sanktionierung wäre mit deutschem Verfassungsrecht nicht vereinbar. Denn das deutsche Rechtssystem baut auf dem Gedanken auf, dass Strafe stets Schuld voraussetzt („nulla poena sine culpa"). Dieses sogenannte Schuldprinzip wird vom Bundesverfassungsgericht als integrationsfester Verfassungsgrundsatz eingeordnet[24] und gilt hiernach nicht nur für das Strafrecht, sondern kann auch im Ordnungswidrigkeitenrecht Geltung beanspruchen.[25]

1. Abstraktes Schulderfordernis

Durch die Verordnung selbst wird ausdrücklich kein Verschuldenserfordernis aufgestellt. Lediglich im Rahmen der Bußgeldzumessung sollen Vorsatz oder Fahrlässigkeit Berücksichtigung finden (vgl. Art. 83 Abs. 2 S. 2 Buchst. b) DS-GVO). Daneben adressiert die Konkurrenzregel des Art. 83 Abs. 3 DS-GVO die Vorsätzlichkeit oder Fahrlässigkeit des Datenschutzverstoßes. Mit Blick hierauf und auf Erwägungsgrund 148 S. 3 DS-GVO, der nur die Vorsätzlichkeit, nicht aber die Fahrlässigkeit als Zumessungskriterium nennt, kann vertreten werden, dass Grundvoraussetzung der fahrlässige Datenschutzverstoß ist.[26] Zudem wird auch auf europäischer Ebene teilweise von der Geltung des Schuldprinzips ausgegangen,[27] das einen vorsätzlich oder fahrlässig begangenen Datenschutzverstoß voraussetzt.[28] Demgegenüber lässt sich für die Ahndung – auch – schuldlos begangener Verstöße anführen, dass die DS-GVO ein Verschuldenserfordernis nicht kodifiziert, obwohl Kommission und Rat dies in den Entwurfsfassungen vorgesehen hatten.[29] Will man von einem Verschuldenserfordernis vorliegend nach dem Maßstab der DS-GVO abweichen, so droht eine Kollision mit dem vorbenannten Schuldprinzip, die allerdings in der Anwendungspraxis durch das regelmäßige Vorliegen von – zumindest – Organisationsverschulden entschärft werden dürfte.[30]

2. Ausführungen des LG Bonn

Nähere Ausführungen des LG Bonn zu einem Verschuldenserfordernis erfolgen nicht. Das Gericht stellt aber jedenfalls fest, dass die Betroffene als Datenverantwortliche den Verstoß schuldhaft begangen hat.[31] Auf diese Weise gibt das LG Bonn zu erkennen, dass es einen verschuldeten Datenschutzverstoß für erforderlich hält.

Im Kontext der Schuld des Verantwortlichen thematisiert das LG Bonn zudem einen möglichen Verbotsirrtum (vgl. § 17 StGB).[32] Das Gericht geht insoweit davon aus, dass die 1&1 Telecom GmbH sich des begangenen datenschutzrechtlichen Verstoßes nicht als solchem bewusst war. Dabei wird darauf verwiesen, dass die in Rede stehende Authentifizierungspraxis der 1&1 Telecom GmbH von Behördenseite in

19 LG Bonn, Urt. v. 11.11.2020 – 29 OWi 1/20 = RDV 2021, 48, Rn. 53.

20 LG Bonn, Urt. v. 11.11.2020 – 29 OWi 1/20 = RDV 2021, 48, Rn. 62.

21 Zur Kritik Paal, RDV 2020, 57, 59 ff.

22 A.A. für Österreich ÖVwGH, Erkenntnis v. 12.05.2020 – Ro 2019/04/0229 = ZD 2020, 463; die Entscheidung bestätigend ÖBVwG, Entscheidung v. 26.11.2020 – W258 2227269-1/14E; a.A. wohl auch das LG Berlin in einem – noch nicht veröffentlichten – Bechl. v. 18.02.2021: Eine juristische Person könne nicht Betroffene in einem Bußgeldverfahren sein.

23 ÖBVwG, Entscheidung v. 26.11.2020 – W258 2227269-1/14E.

24 BVerfG, Beschl. v. 15.12.2015 – 2 BvR 2735/14 = NJW 2016, 1149 Rn. 36.

25 HK DS-GVO/BDSG, Schwartmann/Burkhardt, DS-GVO-BDSG, 2. Aufl. 2020, Anh. zu Art. 83 DS-GVO/§ 41 BDSG Rn. 17.

26 So auch Taeger/Gabel/Moos/Schefzig, DS-GVO – BDSG, 3. Aufl. 2019, Art. 83 DS-GVO Rn. 111.

27 Meyer/Hölscheidt/Eser/Kubiciel, Charta der Grundrechte der Europäischen Union, 5. Aufl. 2019, Art. 48 GRCh Rn. 6.

28 So Auernhammer/Golla, DS-GVO BDSG, 6. Aufl. 2018, Art. 83 DS-GVO Rn. 15.

29 Kühling/Buchner/Bergt, DS-GVO BDSG, 3. Aufl. 2020, Art. 83 DS-GVO Rn. 35.

30 Kühling/Buchner/Bergt, DS-GVO BDSG, 3. Aufl. 2020, Art. 83 DS-GVO Rn. 37.

31 LG Bonn, Urt. v. 11.11.2020 – 29 OWi 1/20 = RDV 2021, 48. Rn. 63.

32 LG Bonn, Urt. v. 11.11.2020 – 29 OWi 1/20 = RDV 2021, 48. Rn. 79.

der Vergangenheit nicht bemängelt worden war.[33] Darüber hinaus habe es hinsichtlich der Anforderungen an die Identifizierung und Authentifizierung von Kunden in Callcentern keine einheitlichen Vorgaben und kaum einschlägige Literatur gegeben.[34] Zwar geht das Gericht von einer Vermeidbarkeit des Verbotsirrtums und damit dessen Irrelevanz im Rahmen der Schuld aus, berücksichtigt den Irrtum aber sodann bei der Strafzumessung (so auch § 17 S. 2 StGB).[35] Die Vermeidbarkeit des Verbotsirrtums begründet das Gericht maßgeblich damit, dass die 1&1 Telecom GmbH ihre Datenschutzpraxis regelmäßig, insbesondere aber jedenfalls in Ansehung der Einführung der DS-GVO, einer – auch rechtlichen – Überprüfung hätte unterziehen müssen, wie sich auch aus Art. 32 Abs. 1 Buchst. d) DS-GVO ergebe.[36]

3. Auswahl milderer Sanktionsmittel Verhältnismäßigkeitsgrundsatz

In diesem Zusammenhang ist ferner die Frage aufgeworfen, ob und inwieweit die DS-GVO im Fall eines Datenschutzverstoßes zur Verhängung eines Bußgeldes verpflichtet. Nach der nationalen Vorschrift des § 47 Abs. 1 S. 1 OWiG, auf die § 41 Abs. 1 S. 1 BDSG verweist, steht die Bußgeldverhängung im pflichtgemäßen (Entschließungs-)Ermessen der Behörden. Danach könnte die entsprechende Behörde also im Rahmen des ihr zustehenden Ermessens selbst entscheiden, ob eine Geldbuße verhängt oder auf die Bußgeldverhängung nach Art. 58 Abs. 2 Buchst. i) DS-GVO i.V.m. Art. 83 DS-GVO verzichtet und sich beispielsweise mit einer Verwarnung gemäß Art. 58 Abs. 2 Buchst. b) DS-GVO begnügt wird. Die indikativische Wortwahl in Art. 83 Abs. 2 S. 1 DS-GVO und Art. 83 Abs. 4 bis 6 DS-GVO sowie Art. 58 Abs. 2 Buchst. i) DS-GVO und Erwägungsgrund 148 S. 1 DS-GVO, die die Bußgelder jeweils zusätzlich oder anstelle von anderen Maßnahmen verhängt wissen wollen, sprechen jedoch gegen die Geltung eines solchen Opportunitätsprinzips[37] und legen vielmehr die Etablierung eines Legalitätsprinzips im Rahmen der DS-GVO nahe.[38]

Vorrangig Berücksichtigung zu finden hat in diesem Kontext zudem der Verhältnismäßigkeitsgrundsatz, der primärrechtlich in Art. 49 Abs. 3, 52 Abs. 1 S. 2 GRCh verankert ist und dessen Geltung bereits Art. 83 Abs. 1 DS-GVO betont. Um diesen Verhältnismäßigkeitsgrundsatz zu wahren, wird die Behörde im Einzelfall von der Bußgeldverhängung absehen können, wenn und soweit andere Mittel zur Gewährung eines hohen Datenschutzniveaus eingesetzt werden können.[39] Dies impliziert auch Erwägungsgrund 148 S. 2 DS-GVO, der eine Verwarnung im Fall eines geringfügigen Verstoßes oder einer unverhältnismäßigen Belastung einer natürlichen Person als milderes Mittel benennt. Beschränkt wird das Ermessen der Behörde schließlich wiederum durch den effet utile-Grundsatz, der ein Absehen von der Bußgeldverhängung nur im Ausnahmefall zulässt.

Das LG Bonn verhält sich zu dieser Problematik zwar nicht ausdrücklich. Aus den fehlenden Ausführungen wird aber keineswegs geschlossen werden können, dass das Gericht von der Geltung des Legalitätsprinzips im Rahmen des Datenschutzbußgeldrechts ausgeht. Vielmehr ist anzunehmen, dass aufgrund der Erheblichkeit des Verstoßes ein Absehen von der Bußgeldverhängung im entscheidungserheblichen Fall von vornherein nicht in Betracht kommen konnte.

IV. Bußgeldzumessung/Maßgebliche Kriterien

Besondere Aufmerksamkeit erfährt das Urteil des LG Bonn mit guten Gründen im Hinblick auf die Bestimmung der Bußgeldhöhe. Während der BfDI noch ein Bußgeld in Höhe von € 9,55 Mio. verhängt hatte,[40] hat das LG Bonn die Sanktion sodann im Ergebnis um rund 90% auf – immer noch durchaus beachtliche – € 900.000 reduziert.

Hintergrund und Maßstab der Bußgeldzumessung durch den BfDI im Falle der 1&1 Telecom GmbH war neben den rechtlichen Rahmenvorgaben der DS-GVO insbesondere das neue Bußgeldkonzept[41] der DSK aus dem Jahr 2019. Dieses Bußgeldkonzept soll eine einheitliche und transparente, für die betroffenen Unternehmen vorhersehbare Bußgeldpraxis schaffen, hat infolge seiner konkreten Ausgestaltung aber auch Kritik erfahren.[42]

1. Ausgangspunkt: Art. 83 DS-GVO

Normativer Ausgangspunkt der Bußgeldzumessung ist Art. 83 Abs. 1 DS-GVO, wonach das durch die zuständige Aufsichtsbehörde verhängte Bußgeld in jedem Einzelfall wirksam, verhältnismäßig und abschreckend sein soll. Neben diesen generell(er)en und im konkreten Einzelfall auslegungsbedürftigen Faktoren[43] werden in Art. 83 Abs. 2 S. 2 DS-GVO eine Reihe von speziellen Kriterien aufgeführt, die bei der Bemessung der Bußgeldhöhe zu berücksichtigen sind. So sollen sowohl tatbezogene (i.e. Art. 83 Abs. 2 S. 2 Buchst. a), b), e), g) DS-GVO) als auch täterbezogene Umstände wie getroffene Präventivmaßnahmen (vgl. Art. 83

33 LG Bonn, Urt. v. 11.11.2020 – 29 OWi 1/20 = RDV 2021, 48, Rn. 79.

34 LG Bonn, Urt. v. 11.11.2020 – 29 OWi 1/20 = RDV 2021, 48, Rn. 79.

35 LG Bonn, Urt. v. 11.11.2020 – 29 OWi 1/20 = RDV 2021, 48, Rn. 80 ff.

36 LG Bonn, Urt. v. 11.11.2020 – 29 OWi 1/20 = RDV 2021, 48, Rn. 81 f.

37 Für die Geltung des Opportunitätsprinzips bei der Entscheidung über die Verhängung einer Geldbuße Paal/Pauly/Frenzel, DS-GVO BDSG, 3. Aufl. 2021, § 41 BDSG Rn. 7.

38 Eingehend zum Wortlautargument Kühling/Buchner/Bergt, DS-GVO BDSG, 3. Aufl. 2020, Art. 83 DS-GVO Rn. 32 ff.

39 So auch Heidelberger Kommentar/Schwartmann/Burkhardt, DS-GVO/BDSG, 2. Aufl. 2020, Anh. zu Art. 83 DS-GVO/§ 41 BDSG Rn. 28 „gestuftes System der Abhilfebefugnisse".

40 Bundesbeauftragter für Datenschutz und Informationsfreiheit, PM vom 09.12.2019, abrufbar unter https://www.bfdi.bund.de/DE/Infothek/Pressemitteilungen/2019/30_BfDIverh%C3%A4ngtGeldbu%C3%9Fe1u1.html (zuletzt abgerufen am 25.02.2021).

41 DSK, Konzept der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder zur Bußgeldzumessung in Verfahren gegen Unternehmen, 14.10.2019.

42 Die nachfolgenden Ausführungen zum Bußgeldkonzept der DSK setzen Überlegungen aus einem Beitrag des Autors zum selben Thema in RDV 2020, 57 fort.

43 Die Art.-29-Datenschutzgruppe verweist insoweit lediglich auf eine durch die aufsichtsbehördliche Praxis und die Gerichte vorzunehmende nähere Begriffsbestimmung, vgl. Art.-29-Datenschutzgruppe, WP 253, Leitlinien für die Anwendung und Festsetzung von Geldbußen im Sinne der Verordnung (EU) 2016/679, angenommen am 3. Oktober 2017, S. 6.

Abs. 2 S. 2 Buchst. d), i), j) DS-GVO) und das Nachtatverhalten (vgl. Art. 83 Abs. 2 S. 2 Buchst. c), f), h) DS-GVO) des Bußgeldadressaten eine Rolle spielen.[44] Die in Art. 83 Abs. 2 S. 2 DS-GVO benannten Zumessungskriterien sind dabei nicht als abschließend zu verstehen, wie sich – unter anderem – aus der Auffangklausel des Art. 83 Abs. 2 S. 2 Buchst. k) DS-GVO ergibt, wonach jegliche anderen erschwerenden oder mildernden Umstände im jeweiligen Fall von Relevanz sein sollen. Zudem wird in Art. 83 Abs. 4 bis 6 DS-GVO im Sinne einer Höchstgrenze festgelegt, dass das Bußgeld insgesamt bis zu € 10 Mio. respektive € 20 Mio. oder – soweit dieser Betrag höher ist – 2 % bzw. 4 % des Jahresumsatzes des betroffenen Unternehmens betragen darf.

2. Die Berechnung nach dem Bußgeldkonzept der DSK

Die Anknüpfung an den (Vor-)Jahresumsatz der betroffenen Unternehmen zur Bestimmung der Bußgeldhöchstgrenze ermöglicht den Aufsichtsbehörden die Verhängung erheblich spürbarer Bußgelder und schafft ein Bedürfnis nach Transparenz sowie Einheitlichkeit bei der Sanktionierung.[45] Diesem Bedürfnis soll im Grundsatz im Wege der Ausarbeitung entsprechender Leitlinien durch den Europäischen Datenschutzausschuss (im Folgenden: EDSA) Rechnung getragen werden (Art. 70 Abs. 1 S. 2 Buchst. k) DS-GVO). Derartige Leitlinien des EDSA existieren aber (noch) nicht.[46] Vor diesem Hintergrund etabliert das Konzept der DSK eine von allen inländischen Datenschutzaufsichtsbehörden anzuwendende[47] Berechnungsmethode für Bußgelder gegenüber Unternehmen. Diese Berechnungsmethode sieht ein fünfstufiges Verfahren vor:[48]

In einem ersten Schritt werden Unternehmen auf Grundlage des Vorjahresumsatzes in eine von vier Größenklassen eingeordnet. Innerhalb dieser Größenklassen erfolgt zudem eine weitere Zuteilung zu einer von insgesamt zwanzig Unterkategorien zwischen „Kleinstunternehmen mit Umsatz von bis zu € 700.000“ und „Großunternehmen mit Umsatz von mehr als € 500 Mio.“ Unter „Umsatz“ versteht die DSK hier den Umsatz der gesamten Unternehmensgruppe und wendet damit den aus dem Unionskartellrecht bekannten funktionalen Unternehmensbegriff[49] an. Den ersten neunzehn dieser Untergruppen wird in einem zweiten Schritt ein mittlerer Jahresumsatz zugeordnet, der sodann durch 360 (Tage) geteilt wird, um in einem dritten Schritt einen mittleren Tagessatz (wirtschaftlicher Grundwert) zu erhalten. Lediglich in der Gruppe der Großunternehmen mit Umsatz von mehr als € 500 Mio. soll der konkrete Jahresumsatz – und nicht etwa der von der DSK festgelegte Mittelwert – als Berechnungsgrundlage für den Tagessatz dienen. Schließlich wird in einem vierten Schritt anhand des Schweregrads der Tat ein Faktor zwischen eins und zwölf bestimmt, mit dem der zuvor ermittelte Tagessatz multipliziert wird. Der entsprechend anzuwendende Faktor richtet sich zum einen danach, ob es sich um einen formellen Verstoß im Sinne von Art. 83 Abs. 4 DS-GVO oder um einen materiellen Verstoß im Sinne von Art. 83 Abs. 5, 6 DS-GVO handelt. Zum anderen finden auf dieser Ebene bei der Bestimmung des Multiplikators erstmals auch die (tatbezogenen) Zumessungskriterien des Art. 83 Abs. 2 S. 2 DS-GVO Berücksichtigung. Im abschließenden fünften Schritt besteht die Möglichkeit, den errechneten Betrag anhand aller sonstiger Umstände des Einzelfalls sowie auch und gerade unter Heranziehung der (täterbezogenen) Kriterien des Art. 83 Abs. 2 S. 2 DS-GVO anzupassen.

3. Ausführungen des LG Bonn

Zur Bestimmung der Bußgeldobergrenze bei der Sanktionierung von Unternehmen spricht sich das LG Bonn unter Verweis auf Erwägungsgrund 150 S. 3 DS-GVO zunächst ausdrücklich für die Verwendung des funktionalen Unternehmensbegriffs aus und befindet sich damit in diesem Punkt auf einer Linie mit der Positionierung der DSK.[50] Festgestellt wird dabei, dass die in Art. 4 Nr. 18 DS-GVO niedergelegte Legaldefinition einem solchen Verständnis zwar widerspreche. Sodann stützt sich das Gericht aber auf einen Vergleich mit anderen Sprachfassungen und insbesondere der englischen Sprachfassung, um die Verwendung des funktionalen Unternehmensbegriffs im Rahmen des Datenschutzbußgeldrechts zu begründen.[51] Als Berechnungsgrundlage für die Bestimmung der Bußgeldobergrenze zieht das LG Bonn nach kartellrechtlichem Vorbild den Jahresumsatz des Unternehmens im letzten abgeschlossenen Geschäftsjahr vor Erlass des Bußgeldbescheides heran.[52]

Hervorzuheben ist, dass das LG Bonn im Rahmen der Bestimmung der Bußgeldhöhe als solcher in erster Linie die einzelfallbezogenen Kriterien des Art. 83 Abs. 2 S. 2 DS-GVO zugrunde legt und diesen eine gegenüber dem Unternehmensumsatz hervorgehobene Bedeutung beimisst. Zwar betont das Gericht, dass der Umsatz als solcher bei der Bußgeldzumessung nicht unberücksichtigt bleiben darf.[53] Die – im Konzept der DSK vorgeschlagene – maßgebliche Anknüpfung an den Unternehmensumsatz und gleichzeitige Zurückdrängung der tatsächlich in Art. 83 Abs. 2 S. 2 DS-GVO aufgeführten Zurechnungskriterien wird aber als prob-

44 Zu dieser Einteilung Behr/Tannen, CCZ 2020, 120, 123 f.

45 Vgl. Erwägungsgrund 150 S. 1 DS-GVO.

46 Der EDSA hat sich bislang lediglich den Leitlinien der Art.-29-Datenschutzgruppe angeschlossen, die aber ihrerseits keine umfassenden Vorgaben enthalten. Siehe hierzu Art.-29-Datenschutzgruppe, WP 253, Leitlinien für die Anwendung und Festsetzung von Geldbußen im Sinne der Verordnung (EU) 2016/679, angenommen am 3. Oktober 2017, S. 4.

47 Das Bußgeldkonzept soll in diesem Sinne nur die Ermessensausübung der deutschen Aufsichtsbehörden binden, nicht hingegen Gerichte oder ausländische Behörden. Vgl. DSK, Konzept der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder zur Bußgeldzumessung in Verfahren gegen Unternehmen, 14.10.2019, S. 1.

48 Ausführlich(er) zur Berechnungsmethode siehe DSK, Konzept der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder zur Bußgeldzumessung in Verfahren gegen Unternehmen, 14.10.2019, S. 3 ff.; Paal, RDV 2020, 57, 58 f.; Timner/Radlanski/Eisenfeld, CR 2019, 782, 782 f.

49 Dazu bereits im Rahmen der Zurechnung des Datenschutzverstoßes vorstehend unter Abschn. II.

50 LG Bonn, Urt. v. 11.11.2020 – 29 OWi 1/20 = RDV 2021, 48, Rn. 85.

51 LG Bonn, Urt. v. 11.11.2020 – 29 OWi 1/20 = RDV 2021, 48, Rn. 86. Zum Streitstand siehe etwa HK, DS-GVO/BDSG, Schwartmann/Burkhardt, DS-GVO/BDSG, 2. Aufl. 2020, Anh. zu Art. 83 DS-GVO/§ 41 BDSG Rn. 9 ff.; Kühling/Buchner/Bergt, DS-GVO BDSG, 3. Aufl. 2020, Art. 83 DS-GVO Rn. 39 ff.

52 LG Bonn, Urt. v. 11.11.2020 – 29 OWi 1/20 = RDV 2021, 48, Rn. 88 ff.

53 LG Bonn, Urt. v. 11.11.2020 – 29 OWi 1/20 = RDV 2021, 48, Rn. 93.

lematisch eingestuft.[54] Als nicht sachgerecht erweise sich eine solche Anknüpfung an den Unternehmensumsatz insbesondere bei schweren Datenschutzverstößen umsatzschwacher Unternehmen und bei leichten Datenschutzverstößen umsatzstarker Unternehmen.[55] Würden die Zumessungskriterien des Art. 83 Abs. 2 S. 2 DS-GVO außer Acht gelassen, drohte die Sanktion nicht (mehr) dem Verhältnismäßigkeitsgrundsatz zu genügen.

Konkret würdigt das LG Bonn daher in seiner Entscheidung den als vergleichsweise gering zu bewertenden Datenschutzverstoß (vgl. Art. 83 Abs. 2 S. 2 Buchst. a) DS-GVO) und die Kategorien personenbezogener Daten, die von dem Verstoß betroffen sind (vgl. Art. 83 Abs. 2 S. 2 Buchst. g) DS-GVO): Sensible Daten hätten durch einen Anruf bei dem Callcenter des Telekommunikationsdienstleisters nicht abgefragt werden können.[56] So wurden den Callcenter-Mitarbeitern bestimmte Daten, wie beispielsweise die Kontoverbindung des Kunden nur unvollständig angezeigt.[57] Andere Daten, wie etwa Daten im Sinne des Art. 9 Abs. 1 DS-GVO, Einzelverbindungsnachweise oder sonstige Verkehrsdaten waren für die Mitarbeiter überhaupt nicht einsehbar und hätten damit auch nicht herausgegeben werden können. Ferner bestand von vornherein keine Gefahr des Massendiebstahls von Kundendaten.[58] Schließlich war es nur in einem Fall zur Schädigung eines Kunden gekommen.[59]

Zu einer Herabsetzung der im Bußgeldbescheid festgesetzten Bußgeldhöhe veranlasst sieht sich das Gericht außerdem durch den Umstand, dass der Datenschutzverstoß nicht vorsätzlich begangen worden sei (s. hierzu Art. 83 Abs. 2 S. 2 Buchst. b) DS-GVO) und dass sich der Telekommunikationsdienstleister hinsichtlich des Schutzniveaus des Authentifizierungsverfahrens in einem (vermeidbaren) Rechtsirrtum befunden habe.[60]

Die umfassende Kooperation mit der Aufsichtsbehörde und die schnelle Reaktion des Telekommunikationsdienstleisters auf die aufgezeigten Lücken im Authentifizierungsverfahren im Wege einer Anpassung des Schutzniveaus werden seitens des Gerichts positiv berücksichtigt (vgl. Art. 83 Abs. 2 S. 2 Buchst. f) DS-GVO).[61] Zudem wird der 1&1 Telecom GmbH zugutegehalten, dass es sich um einen erstmaligen Verstoß handelte (vgl. Art. 83 Abs. 2 S. 2 Buchst. e) DS-GVO).[62] Über die ausdrücklich normierten Zumessungskriterien hinaus bewertet das Gericht den Reputationsschaden, der dem Telekommunikationsdienstleister (fälschlicherweise) entstanden ist, als mildernden Umstand (vgl. Art. 83 Abs. 2 S. 2 Buchst. k) DS-GVO).[63]

4. Stellungnahme

Das Bußgeldkonzept der DSK hat im Schrifttum von verschiedener Seite pointierte Kritik erfahren. An dieser Stelle kann und soll keine detaillierte Auseinandersetzung mit diesen Kritikpunkten erfolgen.[64] Vielmehr werden nachstehend (nur) jene Gesichtspunkte aufgegriffen, die im Kontext des vom LG Bonn entschiedenen Falles relevant wurden.

Zentral ist insoweit die starke – vom LG Bonn zutreffend bemängelte – Fokussierung des Bußgeldkonzepts auf den Umsatz des betroffenen Unternehmens. Die DSK führt an, der Unternehmensumsatz stelle „eine geeignete, sachgerechte und faire Anknüpfung" für die Bußgeldzumessung dar.[65] Während sich die aus der Objektivität und Greifbarkeit des Umsatz-Kriteriums folgenden Vorteile einer Bußgeldzumessung ohne Weiteres erschließen, wiegt gleichwohl schwer, dass sich dieses Kriterium (zu) weit von dem geschriebenen Kriterienkatalog des Art. 83 Abs. 2 S. 2 DS-GVO – und somit vom Wortlaut der Norm – entfernt.[66] Denn der Unternehmensumsatz ist als Kriterium hier normativ gerade nicht genannt, sondern könnte allenfalls unter die sonstigen Milderungs- und Erschwerungsgründe aus Art. 83 Abs. 2 S. 2 Buchst. k) DS-GVO subsumiert werden. Dass eine lediglich als „Auffangkriterium" ausgestaltete Kategorie derart in den Mittelpunkt der Bußgeldzumessung gerückt wird, wie es das Bußgeldkonzept der DSK aktuell vorsieht, ist zumindest problematisch.[67]

Die hierdurch induzierten Schwächen der Berechnungsmethode offenbaren sich auch und gerade in dem vom LG Bonn entschiedenen Fall: So ist die 1&1 Telecom GmbH Konzernangehörige der United Internet AG, deren Umsatz im Jahr 2018 bei € 5,1 Mrd. lag.[68] Ausgehend von diesem Betrag ergibt sich ein mittlerer Tagessatz von € 14,2 Mio., der für die Bußgeldzumessung zugrunde zu legen ist. Selbst bei wohlwollenden Bemühungen der Aufsichtsbehörden, strafmildernde Umstände zu berücksichtigen, lässt sich dieses Ergebnis aufgrund der maßgeblichen Orientierung am Unternehmensumsatz in der weiteren Berechnung nur geringfügig und zudem erst auf letzter Stufe korrigieren. Zutreffend zeigt das LG Bonn auf, dass das DSK-Konzept gerade dann wenig überzeugende Ergebnisse liefert, wenn es sich um schwere Datenschutzverstöße umsatzschwacher Unternehmen oder leichte Datenschutzverstöße umsatzstarker Unternehmen handelt. Die erheblich präformierende Determinierung der Bußgeldhöhe durch den Unternehmensumsatz lässt in diesen Fällen die Tatangemessenheit der Geldbuße in problematischer Weise zurücktreten.

54 LG Bonn, Urt. v. 11.11.2020 – 29 OWi 1/20 = RDV 2021, 48, Rn. 93.

55 LG Bonn, Urt. v. 11.11.2020 – 29 OWi 1/20 = RDV 2021, 48, Rn. 93 ff.

56 LG Bonn, Urt. v. 11.11.2020 – 29 OWi 1/20 = RDV 2021, 48, Rn. 98.

57 LG Bonn, Urt. v. 11.11.2020 – 29 OWi 1/20 = RDV 2021, 48, Rn. 5 ff.

58 LG Bonn, Urt. v. 11.11.2020 – 29 OWi 1/20 = RDV 2021, 48, Rn. 106.

59 LG Bonn, Urt. v. 11.11.2020 – 29 OWi 1/20 = RDV 2021, 48, Rn. 99.

60 LG Bonn, Urt. v. 11.11.2020 – 29 OWi 1/20 = RDV 2021, 48, Rn. 100 ff.

61 LG Bonn, Urt. v. 11.11.2020 – 29 OWi 1/20 = RDV 2021, 48, Rn. 104.

62 LG Bonn, Urt. v. 11.11.2020 – 29 OWi 1/20 = RDV 2021, 48, Rn. 105.

63 LG Bonn, Urt. v. 11.11.2020 – 29 OWi 1/20 = RDV 2021, 48, Rn. 107.

64 Ausführlich(er) hierzu siehe etwa Paal, RDV 2020, 57, 59 ff; Timner/Radlanski/Eisenfeld, CR 2019, 782, 783 ff.

65 DSK, Konzept der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder zur Bußgeldzumessung in Verfahren gegen Unternehmen, 14.10.2019, S. 2.

66 Paal, RDV 2020, 57, 59.

67 So auch Timner/Radlanski/Eisenfeld, CR 2019, 782, 783; Heidelberger Kommentar/Schwartmann/Burkhardt, DS-GVO/BDSG, 2. Aufl. 2020, Anh. zu Art. 83 DS-GVO/§ 41 BDSG Rn. 42.

68 Zur Konzernstruktur s. United Internet, Geschäftsbericht 2018, abrufbar unter https://www.united-internet.de/uploads/tx_unitedinternetpublication/United_Internet_Konzern_2018.pdf (zuletzt abgerufen am 25.02.2021), zum Umsatz s. United Internet, Geschäftsbericht 2018, S. 7, 53, 78.

V. Fazit und Praxisfolgen

Das Urteil des LG Bonn enthält in Abhängigkeit von der jeweiligen Betrachtungsperspektive sowohl erfreuliche als auch weniger erfreuliche Feststellungen. Auf der einen Seite nimmt das Gericht an, dass für Datenschutzverstöße unter Rekurs auf die Grundsätze des unionalen Kartellrechts die Unternehmen für Verstöße ihrer Beschäftigten haften – ohne dass es auf die Vorgaben des Mitgliedstaates zur Zurechnung (i.e. vorliegend § 30 Abs. 1 OWiG) ankommen soll. Auf der anderen Seite bestätigen die Ausführungen des LG Bonn die verschiedentlich geäußerte Kritik an der aktuellen Ausgestaltung des Bußgeldkonzepts der DSK. Hiernach sind die deutschen Datenschutzbehörden aufgefordert, kritisch zu hinterfragen, ob und inwieweit die Ausrichtung am Umsatz zielführend und belastbar ist.

Keinesfalls aber sollte die vom LG Bonn ausgeurteilte Reduzierung des Bußgeldes von den datenschutzrechtlich Verantwortlichen als Signal zur Entspannung missverstanden werden. Vielmehr bleibt es dabei, dass Datenschutzverstöße zunehmend konsequent von den Aufsichtsbehörden verfolgt und sanktioniert werden; die private Rechtsdurchsetzung in Ansehung von auf Art. 82 DS-GVO gestützten Schadensersatzbegehren[69] tritt hinzu.

Unternehmen sind also gut beraten, ihre datenschutzrechtliche Compliance weiterhin stets auf dem neuesten Stand zu halten, worauf auch das LG Bonn in Ansehung der Datenschutzpraxis hinweist – und die weiteren Entwicklungen sorgfältig zu beobachten. Das erste prominente deutsche Gerichtsverfahren zu Bußgeldsanktionen nach der DS-GVO hat aufgezeigt, wo die Streitlinien verlaufen, und es bleibt mit Spannung abzuwarten, was die weitere Rechtsprechung und Behördenpraxis bringen werden. Mit dem aktuellen Beschluss des LG Berlin im Verfahren gegen die Deutsche Wohnen SE manifestieren sich jedenfalls erhebliche Divergenzen zwischen den Rechtsauffassungen der bislang befassten Instanzgerichte.

Prof. Dr. Boris Paal
Inhaber des Lehrstuhls für Bürgerliches Recht und Daten-, Informations- und Medienrecht an der Juristenfakultät der Universität Leipzig

69 Hierzu Paal, MMR 2020, 14.

Tilmann Dittrich/Jan Ippach, LL.M.

Die Beweislast und Darlegungslast bei Ansprüchen nach Art. 82 Abs. 1 DS-GVO

Eine Untersuchung unter Berücksichtigung von Parallelen zum Arzthaftungsrecht

Im Rahmen gerichtlicher Verfahren zu Ansprüchen aus Art. 82 DS-GVO wegen Verstößen gegen die DS-GVO sind die Beweislastregelungen sowohl in der Literatur als auch in der Rechtsprechung umstritten. Erstmals hat nun ein Gericht eine sekundäre Darlegungslast bezüglich der Darlegung des Verstoßes gegen die Verordnung angenommen. Eine solche sekundäre Darlegungslast wurde in Arzthaftungsprozessen durch die Rechtsprechung entwickelt und ist mittlerweile ein wichtiges Element eines Arzthaftungsprozesses. Es stellt sich daher unter anderem die Frage, ob die Annahme einer solchen sekundären Darlegungslast durch die Rechtsprechung auch bei Verstößen gegen Art. 82 Abs. 1 DS-GVO zu erwarten und gerechtfertigt ist. Dieser Frage soll durch die Untersuchung von Gemeinsamkeiten und Unterschieden der Beweislast- und Darlegungslastverteilungen bei Ansprüchen aus dem Arzthaftungsrecht und aus Art. 82 Abs. 1 DS-GVO auf den Grund gegangen werden.

I. Beweis- und Darlegungslast in Arzthaftungsprozessen

Es erfolgt zunächst ein Überblick über die gesetzlichen Regelungen der Beweislastverteilung im Arzthaftungsrecht mit besonderer Betrachtung der Herleitung der sekundären Darlegungslast bezüglich des Behandlungsfehlers.

1. Gesetzliche Regelungen der § § 630a ff. BGB

Das ärztliche Haftungsrecht war zunächst ein hauptsächlich durch Richterrecht geprägter Bereich. Durch das Patientenrechtegesetz 2012 wurden die richterrechtlich entstandenen Prinzipien in den § § 630a ff. BGB ausdrücklich festgelegt.[1]

1 Bergmann/Middendorf, in: Bergmann/Pauge/Steinmeyer, Gesamtes Medizinrecht, 3. Aufl. 2018, BGB, Vorbem. zu §§ 630a Rn. 1.

Ein Schadensersatzanspruch kann daher auf § § 630a Abs. 1, 280 Abs. 1, 241 Abs. 2 BGB gestützt werden. Tatbestandsvoraussetzungen sind hierfür das Vorliegen eines Behandlungsfehlers als Pflichtverletzung, welcher kausal zu einem Schaden geführt hat, was dem Behandelnden schuldhaft vorgeworfen werden kann.

Entsprechend den allgemeinen Beweisregeln des Zivilrechts hat der Patient das Vorliegen eines Behandlungsfehlers, den eingetretenen Schaden und die Kausalität zu beweisen.[2] Für einen Behandlungsfehler aus einem vollbeherrschbaren Risikobereich, der sich durch eine sachgerechte Organisation und Koordinierung minimieren lässt, gilt nach § 630h Abs. 1 BGB eine Beweislastumkehr.[3] Kaum abzugrenzen hiervon ist das Verschulden im Sinne des § 280 Abs. 1 S. 2 BGB, weshalb in den meisten Fällen davon ausgegangen werden kann, dass die Beweislastumkehr sich auch auf dieses erstreckt.[4]

2. Herleitung der sekundären Darlegungslast durch den BGH

Unter der sekundären Darlegungslast versteht sich die prozessuale Situation, dass zwar die eine Partei bezüglich der für sie günstigen Anspruchsvoraussetzungen beweisbelastet ist, jedoch nur ein niedriger Maßstab an die Darlegungstiefe des Vorbringens angesetzt wird, und nun die andere Partei im Sinne des § 138 Abs. 2 ZPO umfassend über die behaupteten Tatsachen darzulegen hat, um nicht Gefahr zu laufen, dass die von der beweisbelasteten Partei vorgebrachten Tatsachen im Sinne des § 138 Abs. 3 ZPO als zugestanden anzusehen sind.[5] Es handelt sich hierbei um keine Beweislastumkehr, sondern um ein Auseinanderfallen der Gewichtung von Beweislast und Darlegungslast.[6]

Der BGH hat eine solche sekundäre Darlegungslast für das Vorliegen eines Behandlungsfehlers aus dem voll beherrschbaren Risikobereich entwickelt. Zuletzt ergingen mehrere Entscheidungen zu Hygienemängeln als voll beherrschbare Risikobereiche in Krankenhäusern, in denen die Voraussetzungen an die sekundäre Darlegungslast konkretisiert wurden.[7] Als erste Voraussetzung wird die Unzumutbarkeit der Darlegung aufgrund unterlegenen Wissens des Patienten angeführt. Im Gegensatz hierzu ist es dem Arzt in der Regel ohne weiteres möglich, die Behandlungsabläufe nachvollziehen und offenlegen zu können. Daher hält der BGH aus Gründen der prozessualen Waffengleichheit die Annahme einer sekundären Darlegungslast für zumutbar.[8]

Für die Praxis relevant ist die Abgrenzung zur Ausforschung.[9] Die Rechtsprechung lässt daher Behauptungen „ins Blaue hinein" nicht genügen, weshalb etwa ein Zeitungsbericht über Hygienemängel im Krankenhaus, der sich aber nicht auf den streitgegenständlichen Behandlungszeitraum bezieht, nicht zur Auslösung der sekundären Darlegungslast genügt.[10] Andererseits lässt die Rechtsprechung ein Vorbringen zu mangelhaften hygienischen Verhältnissen genügen, wenn sie durch Tatsachen substantiiert werden können, wie etwa das Vorliegen von Schimmel im Patientenbad.[11]

II. Beweis- und Darlegungslast bei Ansprüchen nach Art. 82 Abs. 1 DS-GVO

Anhand der einzelnen Anspruchsvoraussetzungen soll nun im Folgenden die jeweilige Beweis- und Darlegungslastverteilung zwischen den Parteien eines Schadensersatzanspruchs nach Art. 82 Abs. 1 DS-GVO untersucht werden.

Zur Veranschaulichung soll der folgende Beispielfall dienen: Ein Patient wird stationär in einem Krankenhaus aufgenommen. Die Patientendaten werden während des Aufenthalts in der digitalen Patientenakte des Krankenhauses gespeichert, worüber der Patient auch umfassend aufgeklärt wird. Einige Jahre später erfährt der Patient aus der Tageszeitung, dass das Krankenhaus jahrelang „schlampig mit den Daten umgegangen sei" und ein Pharmaunternehmen unberechtigt an mangelhaft verschlüsselte Daten gelangt sei.

1. Verstoß gegen die Verordnung

Zunächst muss ein Verstoß gegen die DS-GVO vorliegen. Dass überhaupt eine Datenverarbeitung durch den Anspruchsgegner stattgefunden hat, muss der Anspruchssteller beweisen.[12] Fraglich ist aber, ob nun bezüglich des Verstoßes gegen die Verordnung eine Beweislastumkehr oder eine Verschiebung der sekundären Darlegungslast zulasten des Verarbeitenden eintritt.

a) Beweislastumkehr für den Verstoß gegen die Verordnung

Für eine solche Beweislastumkehr könnte die Rechenschaftspflicht des Art. 5 Abs. 2 DS-GVO i.V.m. der Nachweispflicht nach Art. 24 Abs. 1 S. 1 DS-GVO sprechen.[13] Danach ist der Verantwortliche für die Einhaltung der Vorschriften bei der Verarbeitung von personenbezogenen Daten rechenschafts- und nachweispflichtig.[14] Im Beispielsfall müsste das Krankenhaus also beweisen, dass ihm kein Verstoß gegen die DS-GVO unterlaufen sei.

2 Kern, in: Laufs/Kern/Rehborn, Handbuch des Arztrechts, 5. Aufl. 2019, § 106 Rn. 28.

3 St.Rspr.; vgl. BGH, Urt. v. 20.03.2007 – VI ZR 158/06, NJW 2007, 1682 m.w.N.

4 Spickhoff, in: Spickhoff, Medizinrecht, 3. Aufl. 2018, BGB, § 630h Rn. 2; Deuring, JuS 2020, 489 (490).

5 Stadler, in: Musielak/Voit, ZPO, 17. Aufl. 2020, § 138 Rn. 10a.

6 BGH, Urt. v. 28.08.2018 – VI ZR 509/17, NJW-RR 2019, 17 (20); a.A.: Saenger, in: Saenger, ZPO, 8. Aufl. 2019, § 286 Rn. 71.

7 BGH, Urt. v. 19.02.2019 – VI ZR 505/17, NJW-RR 2019, 467; BGH, Beschl. v. 25.06.2019 – VI ZR 12/17, NJW-RR 2019, 1360; BGH, Beschl. v. 18.02.2020 – VI ZR 280/19, NJW-RR 2020, 720.

8 Prütting, in: MüKo-ZPO, 6. Aufl. 2020, § 286 Rn. 106.

9 OLG Köln, Hinweisbeschl. v. 06.08.2019 – 7 U 119/19, BeckRS 2019, 25896; LG Flensburg, Urt. v. 08.09.2020 – 3 O 375/14, BeckRS 2020, 22423; Katzenmeier, in: Laufs/Katzenmeier/Lipp, Arztrecht, 7. Aufl. 2015, XI Rn. 52.

10 LG Flensburg, Urt. v. 08.09.2020 – 3 O 375/14, BeckRS 2020, 22423.

11 BGH, Urt. v. 19.02.2019 – VI ZR 505/17, NJW-RR 2019, 467 (468).

12 Paal, MMR 2020, 14 (17).

13 Wybitul/Haß/Albrecht, NJW 2018, 113 (116).

14 Geißler/Ströbel, NJW 2019, 3415 (3415).

Eine solch weitreichende Wirkung der Rechenschafts- und Nachweispflichten wird aber von Teilen der Literatur zurecht abgelehnt. Dies wird zum einen damit begründet, dass abweichend vom Untersuchungsgrundsatz des Verwaltungsverfahrensrechts zwar eine Mitwirkungspflicht eines Beteiligten festgelegt werden könne. Dies bedürfe aber einer hinreichenden Bestimmtheit, was im vorliegenden Fall nicht geschehen sei.[15] Außerdem sei eine solche Beweislastumkehr unverhältnismäßig, da dies über den zulässigen Rahmen einer sanktionierenden Wirkung von zivilrechtlichen Ansprüchen hinaus gehen würde.[16]

Eine Beweislastumkehr lässt sich auch nicht aus Art. 82 Abs. 3 DS-GVO herleiten. Denn diese Regelung bezieht sich auf die Verantwortlichkeit für das Schadensereignis und nicht bereits auf den Verstoß.[17] Die Beweislast für den Verstoß verbleibt also entsprechend der allgemeinen Beweisregeln beim Betroffenen.[18]

b) Sekundäre Darlegungslast für den Verstoß gegen die Verordnung

Somit stellt sich die Frage, ob für den vorliegenden Fall die Etablierung einer sekundären Darlegungslast durch die Rechtsprechung zugunsten des Anspruchsstellers für das Vorliegen eines Verstoßes wahrscheinlich ist und ob eine mögliche Etablierung auch gerechtfertigt wäre. Denn die sekundäre Darlegungslast nimmt in Verfahren eine immer bedeutendere Rolle ein.[19]

Eine solche sekundäre Darlegungslast hat bisher in einem lediglich über die Homepage einer Kanzlei veröffentlichten Verfügungsverfahren das LG Hagen[20] angenommen mit der Begründung der Rechenschaftspflicht der Anspruchsgegnerin.

aa) Unzumutbarkeit der Darlegung für den Anspruchssteller

Für den Anspruchssteller könnte der Nachweis eines Verstoßes gegen die Verordnung problematisch sein. Denn es handelt sich zum einen um in der Regel mediale Vorgänge, die für einen Durchschnittsbürger mutmaßlich schwer zu durchschauen und nachzuvollziehen sind,[21] obwohl die Verarbeitung nach Art. 5 Abs. 1 lit. a DS-GVO für die betroffene Person transparent erfolgen muss. Außerdem führt die Bearbeitung und Speicherung der Daten der Anspruchsgegner durch, und die Daten befinden sich somit grundsätzlich in der Sphäre des Verarbeitenden.

Gegen eine solche Unzumutbarkeit könnte man einwenden, es stehe der betroffenen Person nach Art. 15 Abs. 1 DS-GVO ein Auskunftsrecht zu.[22] Diese Argumentation könnte insbesondere auch die extensive Ansicht des LG Dresden[23] zu Art. 15 Abs. 3 DS-GVO unterstützen, welches in dieser Norm sogar eine umfassende Anspruchsgrundlage für eine Auskunftspflicht bezüglich sämtlicher Behandlungsunterlagen gesehen hat.[24] Diese extensive Ansicht bezüglich der Auskunftsrechte aus Art. 15 DS-GVO unterstrich zuletzt auch das AG Bonn mit der Ansicht über Art. 15 Abs. 1 DS-GVO und den Begriff der „personenbezogenen Daten", indem es hierzu nicht nur die Stammdaten zählte, sondern sämtliche Informationen mit Personenbezug.[25]

Dass dieses Argument die Etablierung einer sekundären Darlegungslast nicht zwingend hindern könnte, zeigt das Einsichtsrecht in die Patientenakte aus § 630g Abs. 1 BGB. Denn dieses Einsichtsrecht bestand auch schon vor der Kodifizierung des Richterrechts im Zuge des Patientenrechtegesetzes.[26] Weder das Richterrecht noch das kodifizierte Einsichtsrecht hinderten aber die Rechtsprechung an der Annahme einer sekundären Darlegungslast. Dass die Rechtsprechung aber gerade der Unterschied zwischen einem aktiven Auskunftsrecht im Sinne der DS-GVO und einem passiven Einsichtsrecht im Sinne des § 630g BGB überzeugen könnte, eine Zumutbarkeit des vollständigen Darlegens zulasten des Anspruchsstellers anzunehmen, erscheint fraglich.

bb) Zumutbarkeit des substantiierten Darlegens des Anspruchsgegners

Das zweite Merkmal der sekundären Darlegungslast liegt in der Zumutbarkeit, dass von dem Anspruchsgegner hier ein substantiiertes Vorbringen bezüglich der durch den Anspruchssteller in den Raum gestellten Tatsachen verlangt werden kann.

Dem Verarbeitenden könnte der Nachweis der rechtmäßigen Verarbeitung aufgrund der bereits angesprochenen Rechenschafts- und Nachweispflicht aus Art. 5 Abs. 2 DS-GVO i.V.m. Art. 24 Abs. 1 S. 1 DS-GVO zuzumuten sein. Fest steht zumindest, dass ihm aufgrund dieser Pflichten der Nachweis mit wenig Aufwand gelingen könnte. Denn es bietet sich die Einrichtung eines Datenschutzmanagements bzw. eines Compliance-Systems mit Berücksichtigung der datenschutzrechtlichen Risiken und Regelungen zur Vermeidung von Schadensersatzzahlungen wegen Datenschutzverstößen an,

15 Veil, ZD 2018, 9 (11).

16 Wybitul/Celik, ZD 2019, 529.

17 LG Karlsruhe, Urt. v. 02.08.2019 – 8 O 26/19, ZD 2019, 511 (512); Veil, in: Forgó/Helfrich/Schneider, Betrieblicher Datenschutz, 3. Aufl. 2019, Kapitel 1 Rn. 60.

18 LG Frankfurt, Urt. v. 18.09.2020 – 2-27 O 100/20, GRUR-RS 2020, 24557; LG Frankfurt, Urt. v. 03.09.2020 – 2-03 O 48/19, GRUR-RS 2020, 25111.

19 Prütting, in: MüKo-ZPO, 6. Aufl. 2020, § 286 Rn. 106.

20 LG Hagen, Beschl. v. 09.10.2019 – 10 O 280/19 (abrufbar unter: https://dejure.org/dienste/vernetzung/rechtsprechung?Gericht=LG%20Hagen&Datum=09.10.2019&Aktenzeichen=10%200%20280%2F19; zuletzt abgerufen am: 11.2.2021).

21 Wybitul/Haß/Albrecht, NJW 2018, 113 (116).

22 Wybitul/Haß/Albrecht, NJW 2018, 113 (116); Quaas, in: BeckOK Datenschutzrecht, 34. Edition, Stand: 01.11.2020, Art. 82 Rn. 51.

23 LG Dresden, Urt. v. 29.05.2020 – 6 O 76/20, BeckRS 2020, 19705; Schmidt-Wudy, in: BeckOK Datenschutzrecht, 34. Edition, Stand: 01.11.2020, Art. 15 DS-GVO Rn. 52.2 verweist auf Missbrauchspotential einer weiten Auslegung, hält sie aber für richtig.

24 Ablehnend: Paal, in: Paal/Pauly DS-GVO/BDSG, 3. Aufl. 2021, Art. 15 Rn. 33; Wybitul/Neu/Strauch, ZD 2018, 202 (203).

25 AG Bonn, Urt. v. 30.07.2020 – 118 C 315/19 mit krit. Anm. Laoutoumai, jurisPR-ITR 22/2020 Anm. 6.

26 BGH, Urt. v. 23.11.1982 – VI ZR 222/79, NJW 1983, 328.

wodurch dann bei einem funktionierenden System jederzeit die Einhaltung der Vorschriften belegt werden kann.[27]

Hiergegen spricht aber der gesetzliche Sinn und Zweck der Rechenschafts- und Nachweispflicht. Denn die Rechenschaftspflicht dient den Datenschutzaufsichtsbehörden, wie sich aus Erwägungsgrund 85 der DS-GVO ergibt.[28] Sie vereinfacht die Kontrolle der Einhaltung der datenschutzrechtlichen Vorschriften. Dies verbessert die Effektivität der Kontrollen, die vor Einführung der DS-GVO mitunter daran scheiterten, dass die Verantwortlichen keine Dokumentation von Datenverarbeitungen vorhielten und somit die Beweislage für die Aufsichtsbehörde dünn war.[29] Dass die Nachweispflicht dadurch auch dem Betroffenen mittelbar dient, führt noch nicht dazu, dass ihm hieraus auch subjektive Rechte entstehen.[30] Dies unterstreicht auch, dass es bei der Risikominimierung durch die Rechenschaftspflichten vor allem um die Kontrolle von technischen und organisatorischen Maßnahmen im Sinne des Art. 24 Abs. 1 S. 1, S. 2 DS-GVO geht.[31]

Anders gelagert hingegen ist die Konstellation im Arzthaftungsrecht. Denn der Behandelnde ist aufgrund der gesetzlichen Regelung des § 630f BGB verpflichtet, eine umfassende Dokumentation in einer Patientenakte zu führen. Hierin müssen etwa Einwilligungen in ärztliche Maßnahmen nach § 630f Abs. 2 S. 1 BGB dokumentiert werden. Diese Pflicht trifft den Arzt aufgrund der „ärztlichen Klugheitsregel“,[32] wonach die Dokumentation die Qualität der Behandlung als Gedächtnisstütze steigern soll.[33] Der Gesetzgeber hat aber zudem auch festgelegt, dass die Dokumentationspflicht eine Beweissicherungsfunktion einnimmt, und zwar im Hinblick auf Arzthaftungsprozesse.[34] Es zeigt sich daher, dass die Dokumentationspflicht, wegen der dem Behandelnden die sekundäre Darlegungspflicht auch zuzumuten ist, gerade zugunsten des Anspruchsinhabers in einem Arzthaftungsprozess besteht.

Der Unterschied in den jeweiligen Schutzrichtungen der Vorschriften zeigt sich letztlich auch in den Folgen der Verstöße. Verstößt der Behandelnde gegen die Dokumentationspflicht, so ergeben sich vor allem Folgen für das Arzthaftungsverfahren. Denn § 630h Abs. 3 BGB regelt ausdrücklich eine Beweislastumkehr.[35] Somit bleiben die Folgen im 2-Personen-Verhältnis. Bei einem Verstoß gegen die Rechenschafts- und Nachweispflicht aus Art. 5 Abs. 2 DS-GVO i.V.m. Art. 24 Abs. 1 S. 1 DS-GVO kommt hingegen insbesondere eine Bußgeldsanktion in Betracht.[36] Die Hauptfolgen gehen also aus dem ursprünglichen Anspruchsverhältnis wegen Art. 82 Abs. 1 DS-GVO hinaus.

Es zeigt sich, dass die Annahme einer sekundären Darlegungslast nicht gerechtfertigt ist. Dies würde den Verarbeitenden unzumutbar benachteiligen, da er aufgrund von Nachweis- und Rechenschaftspflichten in der Lage ist, über die Einhaltung der Verordnung durch technische und organisatorische Maßnahmen Auskunft zu geben, die Pflichten aber gerade nicht dem unmittelbaren Schutz des Betroffenen dienen, sondern der Aufsicht durch die zuständige Behörde.

Sofern aber eine sekundäre Darlegungslast in Betracht kommen sollte, muss der von Paal[37] als vermittelnd bezeichnete Lösung von Gola/Piltz[38] zugestimmt werden, dass der Anspruchssteller zumindest das darlegen muss, was eine außenstehende Person, die keinen Einblick in die internen Datenverarbeitungsprozesse hat, erkennen, nachvollziehen und darlegen kann. Dies überspannt nicht die Anforderungen an das Vorbringen, grenzt aber vom Ausforschen ausreichend ab.[39]

Nähme man also eine solche sekundäre Darlegungslast an, würde das im Sinne der vermittelnden Ansicht für den Beispielsfall bedeuten, dass der Patient seine Vermutungen zumindest belegen muss. Der Zeitungsbericht müsste sich also, wie im angesprochenen Hygienefall, zumindest auf einen Zeitraum beziehen, in denen das Krankenhaus überhaupt über Patientendaten des Patienten verfügt hat.[40] Es müsste außerdem naheliegen, dass es sich bei den durch das Unternehmen unzulässig gewonnen Daten um Patientendaten gehandelt habe, damit eine mögliche Betroffenheit des Patienten wahrscheinlich ist.

2. Verschulden für den Verstoß

Nach Art. 82 Abs. 3 DS-GVO besteht die Möglichkeit der Befreiung von der Verantwortlichkeit, indem der Verantwortliche nachweist, alle Sorgfaltspflichten der DS-GVO, die an ihn gestellt werden, erfüllt zu haben.[41] Es wird der Streit geführt, ob hierfür der Sorgfaltsmaßstab des § 276 BGB maßgeblich ist oder ein europarechtlicher Verschuldensmaßstab. Letztlich lassen beide Ansichten aber Vorsatz und jegliche Art der Fahrlässigkeit genügen.[42] Durch Art. 82 Abs. 3 DS-GVO wird die Beweislast für die Verantwortlichkeit auf den Verarbeitenden verlagert.[43] Der Nachweis einer fehlenden Verantwortlichkeit kann durch ein funktionierendes Datenmanagement-System bezüglich der technischen und organisatorischen Maßnahmen belegt werden.[44] Aufgrund des Verhältnismäßigkeitsgrundsatzes bedeutet dies

27 Jung, ZD 2018, 208; Wichtermann, ZD 2016, 421 (422); Schantz, in: BeckOK Datenschutzrecht, 34. Edition, Stand: 01.05.2020, Art. 5 Rn. 39.

28 Wybitul, NJW 2019, 3265 (3268).

29 Veil, ZD 2018, 9 (11 f.).

30 Veil, in: Forgó/Helfrich/Schneider, Betrieblicher Datenschutz, 3. Aufl. 2019, Kapitel 1 Rn. 60; Wybitul, NJW 2019, 3265 (3268).

31 Schantz, in: BeckOK Datenschutzrecht, 34. Edition, Stand: 01.05.2020, Art. 5 Rn. 38; a.A.: Plath, in: Plath, DS-GVO/BDSG, 3. Aufl. 2018, DS-GVO, Art. 24 Rn. 19.

32 Wagner, in: MüKo-BGB, 8. Aufl. 2020, § 630f Rn. 2.

33 Spickhoff, in: Spickhoff, Medizinrecht, 3. Aufl. 2018, BGB, § 630f Rn. 1.

34 BT-Drs. 17/10488, 26; Wagner, in: MüKo-BGB, 8. Aufl. 2020, § 630f Rn. 4.

35 Wagner, in: MüKo-BGB, 8. Aufl. 2020, § 630f Rn. 18.

36 Jaspers/Schwartmann/Hermann, in: Schwartmann/Jaspers/Thüsing/Kugelmann, DS-GVO/BDSG, 2. Aufl. 2020, DS-GVO, Art. 5 Rn. 86.

37 Paal, MMR 2020, 14 (17).

38 Piltz, in: Gola, Datenschutz-Grundverordnung: DS-GVO, 2. Aufl. 2018, Art. 82 Rn. 15.

39 Plath, in: Plath, DS-GVO/BDSG, 3. Aufl. 2018, DS-GVO, Art. 82 Rn. 4.

40 LG Flensburg, Urt. v. 08.09.2020 – 3 O 375/14, BeckRS 2020, 22423 Rn. 21.

41 Wybitul/Haß/Albrecht, ZD 2018, 113 (116).

42 Quaas, in: BeckOK Datenschutzrecht, 33. Edition, Stand: 01.08.2020, Art. 82 Rn. 51; Boehm, in: Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht, 1. Aufl. 2019, DS-GVO, Art. 82 Rn. 22.

43 LG Karlsruhe, Urt. v. 02.08.2019 – 8 O 26/19, ZD 2019, 511 (512); Wybitul, NJW 2019, 3265 (3268).

44 Jung, ZD 2018, 208; Schwartmann/Keppeler/Jacquemain, in: Schwartmann/Jaspers/Thüsing/Kugelmann, DS-GVO/BDSG, 2. Aufl. 2020, DS-GVO, Art. 82 Rn. 34.

für den Beispielsfall, dass bei einem stationären Leistungserbringer im Gesundheitswesen ein umfassenderes Datenmanagement-System erwartet werden kann als beispielsweise von einer ambulanten Arztpraxis, wobei von jeglichen Leistungserbringern zumindest eine ausreichende Verschlüsselung sensibler Gesundheitsdaten verlangt werden kann.[45]

Dies führt unmittelbar auch zum nächsten Problembereich, da zur Einhaltung datenschutzrechtlicher Vorgaben die Zuhilfenahme externer Experten empfehlenswert ist, wenn keine ausreichende Sachkunde vorliegt. Das LG Hamburg[46] entschied jüngst, dass die Einschaltung eines Dienstleisters an der Verantwortlichkeit des Verarbeitenden nichts ändere. Hiergegen könnte aber die Regelung des Art. 82 Abs. 2, Abs. 3 DS-GVO sprechen, wonach auch bei der Einschaltung von Auftragsverarbeitern eine Verantwortlichkeit gegeben sein kann, wovon sich aber Verarbeitende durch den Nachweis der Einhaltung aller Sorgfaltspflichten befreien kann.[47] Etwas anderes ergibt sich auch nicht aus der ohnehin umstrittenen Anwendung des § 831 BGB im vorliegenden Fall. Denn auch dieser enthält eine Exkulpationsmöglichkeit für eine sorgfältige Auswahl.[48] Jedenfalls verbleibt die Beweislast bezüglich der fehlenden Einhaltung von Auswahl- und Überwachungspflichten nach Art. 28 Abs. 1 DS-GVO beim Anspruchssteller.[49]

3. Eintritt eines haftungsbegründenden Schadens

Durch die rechtswidrige Datenverarbeitung muss es zu einem ersatzfähigen Schaden gekommen sein, wofür Art. 82 Abs. 1 DS-GVO sowohl die Möglichkeit des materiellen als auch immateriellen Schadens zulässt. Es handelt sich um jeweils eigenständige Streitgegenstände.[50] Für die Schadenspositionen nennen die Erwägungsgründe 75 und 85 der DS-GVO Beispiele, welche den Anwendungsbereich weit fassen sollen.[51] Problematisch wird der Schadensbegriff aber erst auf der Rechtsfolgenseite.

Als Beispiel für eine immaterielle Schadensposition kommt eine öffentliche Bloßstellung in Betracht durch die Offenlegung von Daten an Dritte ohne das Einverständnis des Betroffenen.[52] Diese Konstellation liegt auch im Beispielsfall vor.

Bezüglich des Schadens befindet sich die Beweislast beim Anspruchssteller.[53]

4. Kausalität zwischen Verstoß und Schaden

Der Begriff der Kausalität muss europarechtlich ausgelegt werden und umfasst auch die reine Mitursächlichkeit.[54] Analog zum kartellrechtlichen Kausalitätsbegriff könnte daher jede Ursächlichkeit ausreichen.[55] Einschränkend wird aber eine typisierende Betrachtung der Vorhersehbarkeit der Schädigung vorgenommen, wodurch außergewöhnliche Abläufe aus der Verursachung ausgenommen werden.[56]

Auch im Rahmen der Kausalität wird eine Beweislastumkehr zulasten des Verarbeitenden diskutiert. Es wird befürchtet, dass die Rechtsprechung eine solche Beweislastumkehr deshalb annehmen könnte, da der Erwägungsgrund 146 der DS-GVO dem Geschädigten einen umfassenden Schadensersatz gewähre und der Betroffene trotz seiner Auskunftsrechte nicht in der Lage sein könnte, die Kausalität nachzuweisen, weshalb zumindest ein abgestufter Maßstab an das Vorbringen bezüglich der Kausalität zu diskutieren sein solle.[57] Diese Ansicht widerspricht aber der durch den Wortlaut der Regelung des Art. 82 Abs. 3 DS-GVO klar begrenzten Anwendung auf das Verschulden.[58]

5. Rechtsfolge: Umfang der Schadensersatzpflicht

Wie bereits erwähnt, sind sowohl materielle als auch immaterielle Schäden ersatzfähig.

a) Materieller Schadensersatz

Bezüglich des materiellen Schadensersatzes sind sämtliche vermögensrechtliche Schadenspositionen denkbar. Dies umfasst insbesondere positive Schäden, aber auch den entgangenen Gewinn.[59] Umstritten und bisher noch nicht letztlich geklärt ist die Entscheidung darüber, ob auch selbst schon der Verlust der Daten einen materiellen Schaden darstellt.[60]

b) Immaterieller Schadensersatz

Deutlich problematischer sind immaterielle Schadenspositionen, bei denen zum letzten Mal besondere Anforderungen an die Darlegungslast gestellt werden müssen. Es stellt sich die Frage nach der Konkretheit und dem Ausmaß des eingetretenen Schadens, wobei für den Schadensumfang die Darlegung einer überwiegenden Wahrscheinlichkeit einer haftungsausfüllenden Kausalität im Sinne des § 287 ZPO genügt.[61]

45 Quaas, in: BeckOK Datenschutzrecht, 34. Edition, Stand: 01.11.2020, Art. 82 Rn. 18.

46 LG Hamburg, Urt. v. 04.09.2020 – 324 S 9/19, BeckRS 2020, 23277.

47 Boehm, in: Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht, 1. Aufl. 2019, DS-GVO, Art. 82 Rn. 24.

48 Wybitul/Haß/Albrecht, NJW 2018, 113 (116); Becker, in: Plath, DS-GVO/BDSG, 3. Aufl. 2018, DS-GVO, Art. 82 Rn. 5b.

49 LG Frankfurt, Urt. v. 18.09.2020 – 2-27 O 100/20, GRUR-RS 2020, 24557.

50 LAG Düsseldorf, Urt. v. 11.03.2020 – 12 Sa 186/19, NZA-RR 2020, 348 (351).

51 Quaas, in: BeckOK Datenschutzrecht, 34. Edition, Stand: 01.11.2020, Art. 82 Rn. 24.

52 LG Frankfurt, Urt. v. 18.09.2020 – 2-27 O 100/20, GRUR-RS 2020, 24557.

53 LAG Düsseldorf, Urt. v. 11.03.2020 – 12 Sa 186/19, NZA-RR 2020, 348 (358); Becker, in: Plath, DS-GVO/BDSG, 3. Aufl. 2018, DS-GVO, Art. 82 Rn. 4.

54 Paal, in: Paal/Pauly DS-GVO/BDSG, 2. Aufl. 2018, Art. 15 Rn. 33; Boehm, in: Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht, 1. Aufl. 2019, DS-GVO, Art. 82 Rn. 13.

55 EuGH, Urt. v. 05.06.2014 – C-557/12, BeckRs 2014, 80953; Wybitul/Haß/Albrecht, NJW 2018, 113 (115).

56 Boehm, in: Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht, 1. Aufl. 2019, DS-GVO, Art. 82 Rn. 13.

57 Wybitul/Haß/Albrecht, NJW 2018, 113 (117).

58 Quaas, in: BeckOK Datenschutzrecht, 34. Edition, Stand: 01.11.2020, Art. 82 Rn. 27.

59 Wybitul/Haß/Albrecht, NJW 2018, 113 (117); Becker, in: Plath, DS-GVO/BDSG, 3. Aufl. 2018, DS-GVO, Art. 82 Rn. 4b.

60 Ablehnend: OLG Dresden, Hinweisbeschl. v. 11.06.2019 – 4 U 760/19, ZD 2019, 567 (568); Paal, MMR 2020, 14 (16) m.w.N.

61 Dickmann, r+s 2018, 345 (351).

Der Erwägungsgrund 85 der DS-GVO nennt als Beispiele für einen immateriellen Schaden die Rufschädigung. Das LG Frankfurt hat als weiteres Beispiel die öffentliche Bloßstellung angeführt, welche durch die Offenlegung von Daten an Dritte ohne das Einverständnis des Betroffenen hervorgerufen werden kann.[62] Der Schadensbegriff muss so gewählt werden, dass er dem Ziel der Verordnung, welcher insbesondere im Schutz personenbezogener Daten liegt,[63] entspricht, wie sich aus Erwägungsgrund 146 der DS-GVO entnehmen lässt. Der Schadensersatz darf daher insbesondere auch ein präventives Element enthalten. Da der immaterielle Schadensersatz aber zumindest mit einer Einschränkung des Schutzes der personenbezogenen Daten zusammenhängen muss, darf nicht jeder Verstoß unmittelbar zu einem Schadensersatz führen.[64] Dies rechtfertigt auch nicht die Präventivwirkung.[65] Daher ist die Einführung einer Bagatellgrenze sinnvoll.[66]

Letztlich muss sich eine benennbare und tatsächliche Persönlichkeitsrechtsverletzung ergeben haben.[67] Erst bei einer ernsthaften Beeinträchtigung, die über die bloße Unannehmlichkeit hinausgeht, soll ein Schadensersatz gewährt werden.[68] Ein bloßes Gefühl des Unbehagens kann und soll keinen Ausgleichsanspruch auslösen können.[69]

Für den Beispielsfall zeigt sich die Brisanz des Verstoßes zum einen in der Intimität der unzulässig gewonnen Gesundheitsdaten und zum anderen auch in der möglichen Missbrauchsgefahr von Gesundheitsdaten durch Dritte.[70] Es würde sich also um eine erhebliche Verletzung des allgemeinen Persönlichkeitsrechts handeln.

II. Fazit/Thesen

1. Im Rahmen des breiten Diskurses über die Beweis- und Darlegungslastverteilungen bei Schadensersatzansprüchen nach Art. 82 Abs. 1 DS-GVO darf sich die Gefahr der uferlosen Ausweitung des Schadensersatzanspruchs hin zu einer Gefährdungshaftung nicht verwirklichen, die vom Verordnungsgeber nicht intendiert war.
2. Das Mittel der Beweislastumkehr außerhalb des ausdrücklichen Anwendungsbereichs nach Art. 82 Abs. 3 DS-GVO muss restriktiv eingesetzt werden.
3. Die aus dem Arzthaftungsrecht bekannte Figur der sekundären Darlegungslast verlangt zum einen den schwierigen Nachweis der günstigen Tatsache für den Anspruchssteller, zum anderen dementsprechend einen zumutbaren Nachweis der Tatsache für den Anspruchsgegner.
4. Im Unterschied zum Arzthaftungsrecht ist es für den Anspruchsgegner entgegen der Ansicht des LG Hagen als unzumutbar anzusehen, den Nachweis der rechtmäßigen Verarbeitung vorzubringen, da die Vorschriften, die ihm dies zwar ermöglichen würden, nicht dem Schutz des Anspruchsstellers dienen.
5. Als Stellglied zur Eindämmung einer möglichen Gefährdungshaftung stellt ein immaterieller Schadensersatzanspruch auf ernsthafte Beeinträchtigungen des Persönlichkeitsrechts des Betroffenen ab.

Tilmann Dittrich, LL.M.
Doktorand an einem Lehrstuhl für Strafrecht an der HHU Düsseldorf, Wissenschaftlicher Mitarbeiter der Kanzlei Prof. Halbe & Partner in Köln, Im Mediapark 6A, 50670 Köln; koeln@medizin-recht.com

Jan Ippach, LL.M.
Rechtsanwalt der Kanzlei Prof. Halbe & Partner in Köln, Im Mediapark 6A, 50670 Köln.

62 LG Frankfurt, Urt. v. 18.09.2020 – 2-27 O 100/20, GRUR-RS 2020, 24557.

63 Erwägungsgrund 2 der DS-GVO.

64 LG Hamburg, Urt. v. 04.09.2020 – 324 S 9/19, BeckRS 2020, 23277.

65 LG Karlsruhe, Urt. v. 02.08.2019 – 8 O 26/19, ZD 2019, 511 (512).

66 OLG Dresden, Hinweisbeschl. v. 11.06.2019 – 4 U 760/19, ZD 2019, 567 (568); Wybitul/Brams, CR 2020, 571 (575); a.A.: ArbG Düsseldorf, Urt. v. 05.03.2020 – 9 Ca 6557/18, BeckRS 2020, 11910.

67 LG Karlsruhe, Urt. v. 02.08.2019 – 8 O 26/19, ZD 2019, 511 (512); Erwägungsgrund 146 S. 6 der DS-GVO; Frenzel, in: Paal/Pauly DS-GVO/BDSG, 2. Aufl. 2018, Art. 82 Rn. 10.

68 OLG Dresden, Hinweisbeschl. v. 11.06.2019 – 4 U 760/19, ZD 2019, 567 (568); Paal, MMR 2020, 14 (16); Halbe/Ippach, in: Dochow/Dörfer/Halbe/Hübner/Ippach/Schröder/Schütz/Strüve, Datenschutz in der ärztlichen Praxis, 1. Aufl. 2019, S. 190.

69 AG Frankfurt, Urt. v. 10.07.2020 – 385 C 155/19 (70), BeckRS 2020, 22861.

70 Dickmann, r+s 2018, 345 (354).

Sebastian Lottkus

Die „Bestandsdatenauskunft II“-Entscheidung des BVerfG[1]

Zugleich eine Analyse der jüngeren konsolidierenden Rechtsprechung des BVerfG zu den verfassungsmäßigen Verhältnismäßigkeitsanforderungen bei Eingriffsbefugnissen der Sicherheitsbehörden

Die Bestandsdatenauskunft II-Entscheidung des BVerfG stellt ein weiteres Kapitel der Prüfung von Eingriffsbefugnissen der Sicherheitsbehörden insbesondere im Hinblick auf das Grundrecht auf informationelle Selbstbestimmung sowie das Telekommunikationsgrundrecht dar. Sie steht damit sowohl im Zusammenhang mit den bereits länger zurückliegenden Entscheidungen zum großen Lauschangriff[2], zu Telekommunikations-Verbindungsdaten,[3] zur Online-Durchsuchung[4] sowie zur Bestandsdatenauskunft I,[5] als auch mit den jüngeren Entscheidungen zum BKAG[6] sowie zu Kennzeichenkontrollen[7] und den Befugnissen des BND.[8]

Die Entscheidung erklärt einige Übermittlungsbefugnisse von Telekommunikationsanbietern sowie mehrere damit korrespondierende Abrufbefugnisse verschiedener Sicherheitsbehörden für mit dem Grundgesetz unvereinbar. Dies stellt bereits für sich einen weiteren wichtigen Schritt hin zur verfassungskonformen Ausgestaltung der Befugnisse der Sicherheitsbehörden dar. Der ungleich größere Verdienst der Entscheidung liegt jedoch in der Fortsetzung der insbesondere mit dem BKAG-Urteil begonnenen Zusammenfassung und Konsolidierung[9] der bisherigen Rechtsprechung des Gerichts zu Eingriffsbefugnissen der Sicherheitsbehörden in die o. g. Grundrechte. Dementsprechend ist Ziel dieses Beitrags nicht nur, die Entscheidungen des Gerichts in der Sache darzustellen (unten Teil III.)[10], sondern diese vor allem in die zuvor (Teil I.) dargestellten Grundzüge der konsolidierenden Konkretisierungen der Entscheidung einzuordnen.

I. Aus der Entscheidung ableitbare konsolidierende Grundzüge zur Verhältnismäßigkeitsprüfung

Aus den Ausführungen des Gerichts im Zusammenhang mit den konkreten Feststellungen der Entscheidung ergeben sich wichtige grundsätzliche Erkenntnisse. Die Entscheidung gibt zumindest in dieser Klarheit erstmals ein zusammenfassendes Bild der einzelnen Schritte der Prüfung von Eingriffsbefugnissen der Sicherheitsbehörden auf Vereinbarkeit mit dem verfassungsrechtlichen Grundsatz der Verhältnismäßigkeit und der zwischen diesen bestehenden Wechselwirkungen.

a) Ausgangspunkt jeder Prüfung einer Eingriffsbefugnis von Sicherheitsbehörden ist zunächst deren Eingriffsgewicht. Dies meint den Umfang und die Schwere, mit der eine Maßnahme einer Sicherheitsbehörde in Grundrechte eingreift. Das Eingriffsgewicht bestimmt sich nach Art, Umfang und denkbarer Verwendung der personenbezogenen Daten sowie der Gefahr ihres Missbrauchs. Zu berücksichtigen ist dabei unter anderem, wie viele Grundrechtsträger wie intensiven Beeinträchtigungen ausgesetzt sind und unter welchen Voraussetzungen dies geschieht, insbesondere, ob diese Personen hierfür selbst einen Anlass gegeben haben.[11] Zusammengefasst sind also die Zahl der Betroffenen sowie die Intensität ihrer Beeinträchtigungen maßgeblich. Die Heimlichkeit einer Maßnahme erhöht das Eingriffsgewicht. Dabei sind Art und Umfang der Datenverwendung nicht allein danach zu beurteilen, welche Intensität die Datenverarbeitung der Sicherheitsbehörden hat. Miteinzubeziehen ist auch, wenn – wie bei der Bestandsdatenauskunft – andere Stellen verpflichtet werden, besonders eingriffsintensive Maßnahmen als Vorarbeit für eine polizeiliche Datenverarbeitung durchzuführen[12].[13]

b) Gemessen am Eingriffsgewicht sind im nächsten Schritt entsprechende Eingriffsschwellen[14] für das Einschreiten der Sicherheitsbehörden vorzusehen. Dies meint Tatbestands-Voraussetzungen, an die eine Datenverarbeitung geknüpft ist. Dabei dürfen Datenerhebungen durch Sicherheitsbehörden nur bei einem auf tatsächliche Anhaltspunkte gestützten Eingriffsanlass erfolgen. Auch Erhebungen von Daten, deren Aussagekraft und Verwendungsmöglichkeiten begrenzt sind, dürfen nicht „ins Blaue hinein“ zugelassen werden. Die Schaffung eines offenen Datenvorrats für vielfältige und ohne Eingriffsanlass begrenzte Verwendungen im gesamten einer Behörde zugewiesenen Aufgabenbereich ist unzulässig. Zur Vermeidung reichen Beschränkungen auf den Einzelfall und einen konkreten Zweck allein nicht aus.

1 Beschluss vom 27.05.2020, 1 BvR 1873/13 und 1 BvR 2618/13 – Im Folgenden: Bestandsdatenauskunft II.

2 BVerfGE 109, 279.

3 BVerfGE 115, 166.

4 BVerfGE 120, 274.

5 BVerfGE 130, 151 (im Folgenden Bestandsdatenauskunft I).

6 BVerfGE 141, 220 (im Folgenden BKAG-Urteil).

7 BVerfGE 150, 244 und 150, 309.

8 Urteil v. 19.05.2020 – 1 BvR 2835/17.

9 Zur Konsolidierungsfunktion des BKAG-Urteils: Pressemitteilung des BVerfG Nr. 19/2016 vom 20.04.2016 und BVerfGE 141, 220 Rn. 292.

10 Hierzu auch bereits Graulich, Bestandsdatenauskunft II – Doppeltüren-Modell und Verhältnismäßigkeitsgrundsatz, NVwZ-Beilage 2020, 47; Löffelmann, Regelungen zur Bestandsdatenauskunft verfassungswidrig (Bestandsdatenauskunft II), GSZ 2020, 182.

11 Bestandsdatenauskunft II, Rn. 129.

12 Beispielsweise die Auswertung von Verkehrsdaten durch Telekommunikationsanbieter zur Ermittlung einer zu beauskunftenden dynamischen IP-Adresse, die selbst nur ein Bestandsdatum darstellt.

13 Bestandsdatenauskunft II, Rn. 99.

14 Synonym teilweise auch „Einschreitschwellen“ – vgl. bspw. BVerfGE 120, 274, Rn. 253.

Zur Gefahrenabwehr ist danach grundsätzlich eine im Einzelfall vorliegende konkrete Gefahr im Sinne der polizeirechtlichen Generalklauseln erforderlich, wobei der Gefahrenverdacht mit umfasst ist. Noch ausreichend wäre auch eine Formulierung, wonach eine im Gesetz ausreichend bestimmte Maßnahme zulässig ist, wenn sie zur Aufgabenwahrnehmung im Einzelfall erforderlich ist, da dies eine Auslegung dahingehend ermöglicht, dass die Erforderlichkeit nur dann gegeben ist, wenn eine konkrete Gefahr vorliegt.[15] Unter bestimmten Voraussetzungen können Eingriffsschwellen jedoch auch abgesenkt werden (s. dazu näher unter I. d).

Bezogen auf die Strafverfolgung reicht das Vorliegen eines Anfangsverdachts. Vage Anhaltspunkte oder Vermutungen reichen demgegenüber nicht aus. Eine unterhalb des Anfangsverdachts liegende Eingriffsschwelle zur Vornahme grundrechtsrelevanter Eingriffe kann nicht genügen, da ansonsten das Kriterium der Tatsachenbezogenheit der Einschreiteschwelle aufgegeben würde. Immerhin sind für einen Anfangsverdacht bereits lediglich zureichende tatsächliche Anhaltspunkte ausreichend, dass eine Person, eine (bestimmte) Straftat begangen haben könnte.[16] Noch ausreichend wäre dagegen eine Formulierung, wonach eine im Gesetz ausreichend bestimmte Maßnahme zulässig ist, wenn sie zur Aufgabenwahrnehmung erforderlich ist, da dies eine Auslegung dahingehend ermöglicht, dass die Erforderlichkeit nur dann gegeben ist, wenn zumindest ein Anfangsverdacht vorliegt.[17]

Eingriffsschwellen sind nur für die erstmalige Verwendung von Daten durch Sicherheitsbehörden erforderlich. Sie müssen somit von einer Rechtsgrundlage zur Gefahrenabwehr oder Strafverfolgung immer dann vorgegeben sein, wenn die Rechtsgrundlage zur erstmaligen Erhebung durch die Sicherheitsbehörden ermächtigt. Dazu gehört auch, wenn die Daten zwar bereits bei anderen Stellen vorhanden sind, die in Rede stehende Vorschrift jedoch Sicherheitsbehörden erstmalig ermächtigt, diese Daten zu verarbeiten. Eingriffsschwellen müssen danach grundsätzlich nicht erfüllt sein, wenn die Nutzung von bei den Sicherheitsbehörden vorhandenen Daten zum Schutz derselben Rechtsgüter und im Rahmen derselben Aufgabenstellungbei als bloßer Spurenansatz erlaubt wird.[18]

c) Das Eingriffsgewicht der konkret in Rede stehenden Maßnahme bestimmt über das Vorhandensein von Einschreiteschwellen hinaus zudem maßgeblich, welche Anforderungen an den Rechtsgüterschutz mindestens zu stellen sind.[19] Der Gesetzgeber muss dabei im Bereich der Gefahrenabwehr und der Strafverfolgung ab einer bestimmten Schwere des Eingriffsgewichts entweder die zu schützenden Rechtsgüter selbst konkret benennen oder zumindest das erforderliche Gewicht normenklar festhalten.[20] Soweit die Gefahrenabwehr auf die Verhütung von Straftaten bezogen ist, muss der Gesetzgeber abschließend festlegen, welche Straftatbestände hiervon umfasst sein sollen. Er kann dabei auf bestehende Kataloge zurückgreifen oder einen eigenen Katalog schaffen, etwa um Straftaten zu erfassen, für die die jeweilige Maßnahme besondere Bedeutung hat. Die Qualifizierungsstufe einer Straftat – beispielsweise als schwer oder besonders schwer – muss dabei in der Strafnorm einen objektivierten Ausdruck finden. Dies kann beispielsweise durch Angabe des Strafrahmens erfolgen. Eine Generalklausel oder die lediglich pauschale Verweisung auf nicht näher eingegrenzte Straftaten reicht hingegen nicht aus.[21] Lediglich bei Maßnahmen von gemäßigtem Eingriffsgewicht kann eine Festlegung besonderer Anforderungen an den Rechtsgüterschutz entbehrlich sein.[22] Solche Maßnahmen können bei Vorliegen hinreichender Eingriffsschwellen zum Schutz jeglicher Rechtsgüter verhältnismäßig sein.

Bei den Nachrichtendiensten können sich die hinreichenden Anforderungen an den Rechtsgüterschutz aus den jeweils in Bezug genommenen Aufgaben der Dienste ergeben. Soweit diese im Schutz entsprechend gewichtiger Rechtsgüter oder vergleichbar gewichtiger öffentlicher Interessen bestehen, ist eine darüber hinausgehende ausdrückliche Regelung von Anforderungen an den Rechtsgüterschutz entbehrlich.[23]

Eine Kategorisierung, in welche unterschiedlichen Stufen es das Eingriffsgewicht von Maßnahmen unterteilt und welche Anforderungen an den Rechtsgüterschutz im Bereich der Gefahrenabwehr bzw. im Bereich der Strafverfolgung in Abhängigkeit der Stufe des Eingriffsgewichts jeweils mindestens zu stellen sind, lässt sich der Rechtsprechung des BVerfG bisher noch nicht abschließend entnehmen. Jedenfalls ausgemacht werden können bereits die Eingriffsstufen „gemäßigtes Eingriffsgewicht“,[24] „erhöhtes Eingriffsgewicht“,[25] „erhebliches Eingriffsgewicht“,[26] „besonders schweres Eingriffsgewicht“[27] und „außerordentliches Eingriffsgewicht“.[28] Eine Maßnahme mit gemäßigtem Eingriffsgewicht verlangt über die Festschreibung qualifizierter Eingriffsschwellen hinaus keine gesteigerten Anforderungen an den Rechtsgüterschutz.[29] Maßnahmen mit erhöhtem Eingriffsgewicht verlangen demgegenüber mindestens den Schutz von Rechtsgütern von hervorgehobenem Gewicht bzw. die Vermeidung entsprechend schwerwiegender Straftaten. Im Bereich der Strafverfolgung müssen sie mindestens der Verfolgung von Straftaten von hervorgehobener Bedeutung dienen.[30] Maßnahmen von erheblichem Eingriffsgewicht müssen zu ihrer Rechtfertigung jeweils auf Gründe gestützt werden, die dem Schutz von Rechtsgütern von zumindest erheblichem Gewicht oder sonst einem vergleichbar

15 Bestandsdatenauskunft II, Rn. 157.

16 Bestandsdatenauskunft II, Rn. 152 und BVerfGE 112, 348, 386 sowie 117, 244, 263.

17 Bestandsdatenauskunft II, Rn. 157.

18 BKAG-Urteil, Rn. 280 f.

19 Bestandsdatenauskunft II, Rn. 148 f., 175 f. und BKAG-Urteil, Rn. 112.

20 Bestandsdatenauskunft II, Rn. 180.

21 Bestandsdatenauskunft II, Rn. 181 m.w.N.

22 Bestandsdatenauskunft II, Rn. 146.

23 Bestandsdatenauskunft II, Rn. 240.

24 Bestandsdatenauskunft II, Rn. 138.

25 Bestandsdatenauskunft II, Leitsatz 4.

26 BVerfGE 150, 244, Rn. 96.

27 BKAG-Urteil, Rn. 151 und Urteil v. 19.05.2020 – 1 BvR 2835/17, Rn. 146.

28 BKAG-Urteil, Rn. 283.

29 Bestandsdatenauskunft II, Rn. 146.

30 Bestandsdatenauskunft II, Rn. 178.

gewichtigen öffentlichen Interesse dienen.[31] Besonders schwere Eingriffe sind zum Schutz überragend wichtiger Gemeinwohlinteressen sowie zur Verhütung und Verfolgung entsprechend schwerwiegender Straftaten zulässig.[32]

Eine Kategorisierung der Eingriffsgewichtsstufen fällt bislang auch deshalb schwer, weil das Gericht die Bezeichnung der genannten Eingriffsstufen nicht durchgehend verwendet, sondern teilweise auch mit Synonymen arbeitet. So stellt die manuelle Bestandsdatenauskunft nach dem BVerfG einerseits eine Maßnahme von „gemäßigtem Gewicht" dar.[33] An anderer Stelle bezeichnet es das Eingriffsgewicht jedoch auch als „weniger gewichtig"[34] bzw. spricht von einem „nicht sehr großen Eingriffsgewicht".[35] Diesbezüglich bietet sich daher sowohl eine genauere Analyse der bisherigen Rechtsprechung an, die den Rahmen dieses Beitrags jedoch sprengen würde, als auch eine fortgesetzte Konsolidierung durch das Gericht.

d) Besondere Klarheit bringt die Bestandsdatenauskunft II-Entscheidung jedoch in das Verhältnis der Anforderungen an den Rechtsgüterschutz zu möglichen Absenkungen der Anforderungen an den Kausalverlauf und die zu fordernde Tatsachengrundlage im Bereich der Gefahrenabwehr. Erfolgte die entsprechende Darstellung in der BKAG- und früheren Entscheidungen noch eher zusammenhanglos, ist die Bestandsdatenauskunft II-Entscheidung hier erfreulich klar. Die Absenkung der Anforderungen an den Kausalverlauf und die zu fordernde Tatsachengrundlage stellen Absenkungen der Eingriffsschwelle dar. Abweichend vom Grundsatz[36], kann die Eingriffsschwelle im Gefahrenabwehrbereich unter besonderen Voraussetzungen auch unterhalb einer konkreten Gefahr angesetzt werden.[37]

Je gewichtiger das gefährdete Rechtsgut ist und je weitreichender es bei Gefahreintritt beeinträchtigt würde, desto geringere Anforderungen müssen an den Grad der Wahrscheinlichkeit und die Tatsachengrundlage gestellt werden.[38] Allerdings muss stets gewährleistet bleiben, dass Annahmen und Schlussfolgerungen einen konkret umrissenen Ausgangspunkt im Tatsächlichen haben. Die Tatsachen müssen dafür zum einen den Schluss auf ein wenigstens seiner Art nach konkretisiertes und zeitlich absehbares Geschehen zulassen, zum anderen darauf, dass bestimmte Personen beteiligt sein werden, über deren Identität zumindest so viel bekannt ist, dass die Überwachungsmaßnahme gezielt gegen sie eingesetzt und weitgehend auf sie beschränkt werden kann.[39] Eine solche vom Gericht sogenannte (hinreichend) konkretisierte Gefahr liegt danach auch dann noch vor, wenn sich der zum Schaden führende Kausalverlauf noch nicht mit hinreichender Wahrscheinlichkeit vorhersehen lässt, jedoch bereits bestimmte Tatsachen auf eine im Einzelfall drohende Gefahr hinweisen.

Die Eingriffsschwelle und die Anforderungen an den Rechtsgüterschutz stehen dabei allerdings in einem Wechselverhältnis.[40] Wenn die Anforderungen an die Tatsachenebene unterhalb der Schwelle einer konkreten Gefahr verringert werden, müssen die Anforderungen an den Rechtsgüterschutz im Gegenzug über das rein nach dem Eingriffsgewicht Erforderliche hinaus in verhältnismäßiger Weise erhöht werden.[41] Je stärker die Anforderungen an den Rechtsgüterschutz über das rein für die Kompensation des Eingriffsgewichts Erforderliche hinaus ausgeprägt sind, umso eher erlauben sie Absenkungen der Eingriffsschwellen durch Ausweitungen des Kausalverlaufs oder eine Absenkung der Anforderungen an die Tatsachengrundlage. Umgekehrt steigen bei einem geringen Gewicht des gefährdeten Rechtsguts die Anforderungen an die Prognosesicherheit sowohl hinsichtlich des Grades der Gefährdung (Wahrscheinlichkeit) als auch hinsichtlich ihrer Intensität. Zur Bestimmung der Anforderungen an den Rechtsgüterschutz ist daher stets das Eingriffsgewicht der konkreten Maßnahme zu berücksichtigen. Während der Absenkung von Eingriffsschwellen bei tief in die Privatsphäre eingreifenden Maßnahmen deutliche Grenzen gesetzt sind, bestehen bei weniger gewichtigen Eingriffen auch weiterreichende Gestaltungsmöglichkeiten.[42] Zum Schutz herausgehobener Rechtsgüter wie etwa zur Verhütung terroristischer Straftaten, können die Anforderungen an den Kausalverlauf allerdings sogar soweit abgesenkt werden, dass zwar noch kein seiner Art nach konkretisiertes und zeitlich absehbares Geschehen erkennbar ist, jedoch zumindest das individuelle Verhalten einer Person die konkrete Wahrscheinlichkeit begründet, dass sie solche Straftaten in überschaubarer Zukunft begehen wird.[43]

Danach stellt sich das Kriterium der Anforderungen an den Rechtsgüterschutz als die wesentliche Stellschraube heraus, mit der sowohl das Eingriffsgewicht einer Maßnahme als auch das Absenken der Eingriffsschwellen ausgeglichen werden kann.

Zwar ist hier eine gewisse Systematik in der Rechtsprechung des Gerichts zu erkennen. So hält es bei der Bestandsdatenabfrage mittels IP-Adressen, wenn nur eine hinreichend konkretisierte Gefahr vorliegt, als Anforderung an den Rechtsgüterschutz beispielsweise den Schutz von zumindest besonders gewichtigen Rechtsgütern für notwendig.[44] Genauso hohe Anforderungen an den Rechtsgüterschutz verlangt das Gericht bei einer konkreten Gefahr sonst nur bei Maßnahmen von besonders schwerem Eingriffsgewicht.[45] Andererseits dürften sich die komplexen Erwägungen im verfassungsrechtlichen Bereich einer ganz strengen Schematik entziehen, wonach bspw. bei einer hinreichend konkretisierten Gefahr im Gefahrenabwehrbereich die Anforderungen an den Rechtsgüterschutz immer einem X Stufen höheren Eingriffsgewicht entsprechen müssen. Dies wird in

31 BVerfGE 150, 244, Rn. 99.
32 BKAG-Urteil, Rn. 169.
33 Bestandsdatenauskunft II, Leitsatz 4.
34 Bestandsdatenauskunft II, Rn. 150.
35 Bestandsdatenauskunft II, Rn. 145.
36 Vgl. oben I. b.) (= konkrete Gefahr bzw. Anfangsverdacht).
37 Bestandsdatenauskunft II, Rn. 147.
38 Bestandsdatenauskunft II, Rn. 147.
39 Bestandsdatenauskunft II, Rn. 147 f. und BKAG, Rn. 112.
40 Bestandsdatenauskunft II, Rn. 179.
41 Bestandsdatenauskunft II, Rn. 180.
42 Bestandsdatenauskunft II, Rn. 149 und BKAG-Urteil, Rn. 104.
43 Bestandsdatenauskunft II, Rn. 147 f. und BKAG-Urteil, Rn. 112.
44 Bestandsdatenauskunft II, RN. 180.
45 BKAG-Urteil, Rn. 151 und 156.

der Entscheidung daran deutlich, dass das Gericht in seine diesbezüglichen Erwägungen auch einbezieht, dass es sich bei der Bestandsdatenauskunft um eine Maßnahme von großer Bedeutung für eine effektive Aufgabenwahrnehmung handelt.[46] Diese zusätzliche Erwägung stellt somit eine ergänzende Stellschraube für die Feinjustage der Verhältnismäßigkeitsprüfung dar. Bei einer ähnlich geregelten Maßnahme ohne derartige Bedeutung mögen somit auch noch höhere Anforderungen an den Rechtsgüterschutz erforderlich sein, wenn sie schon bei einer nur hinreichend konkretisierten Gefahr angewendet werden können soll.

Im Bereich der Strafverfolgung ist anders als im Bereich der Gefahrenabwehr eine derartige Absenkung der Eingriffsschwelle unterhalb der Stufe des Anfangsverdachts unzulässig. Die Annahme eines Anfangsverdachts setzt bereits lediglich das Vorliegen zureichender tatsächlicher Anhaltspunkte für eine Straftat voraus. Solche tatsächlichen Anhaltspunkte liegen hinsichtlich ihrer Aussagekraft noch unter den für manche Ermittlungsmaßnahmen geforderten „bestimmten Tatsachen“, weshalb der Anfangsverdacht bereits die Verdachtsstufe mit den geringsten in der Strafprozessordnung vorgesehenen tatsächlichen Voraussetzungen ist. Würden die Voraussetzungen noch weiter zurückgenommen, wären nur noch vage Anhaltspunkte gefordert.[47]

f) Darüber hinaus können bei Maßnahmen von hohem Eingriffsgewicht oder bei einer erheblichen Absenkung der Eingriffsschwellen als weiterer Ausfluss des Verhältnismäßigkeitsgrundsatzes neben qualifizierten Eingriffsschwellen und hinreichenden Anforderungen an den Rechtsgüterschutz zusätzliche gesetzgeberische Begleitmaßnahmen zur Wahrung der Verhältnismäßigkeit erforderlich sein.[48] Diese unterteilt das BVerfG in verschiedene Kategorien.

Hierzu gehören Regelungen

- zur Transparenz (inkl. Dokumentationspflichten und Berichtspflichten gegenüber Parlament und Öffentlichkeit),[49]
- zum individuellen Rechtsschutz (u.a. Benachrichtigungspflichten),[50]
- zur aufsichtlichen Kontrolle (Datenschutzaufsicht, behördlicher Datenschutzbeauftragter, fachliche Aufsicht in Form einer Behördenleiteranordnung)[51] und zur vorherigen Kontrolle (Richtervorbehalt)[52] sowie
- zur Datensicherheit, zur weiteren Datennutzung und -löschung.[53]

Diese zusätzlichen Anforderungen können die Einhaltung verhältnismäßiger Vorgaben allerdings nur sichern, nicht aber diese Vorgaben ersetzen.[54]

II. Ergänzungen zum Grundsatz der Zweckbindung und dem Prinzip der Doppeltüre

Die Befugnisse zum Datenabruf müssen jedoch nicht nur für sich genommen verhältnismäßig sein, sondern sind – aus Gründen der Normenklarheit – auch an die in den Übermittlungsregelungen begrenzten Verwendungszwecke gebunden. Dies gilt auch, soweit diese verfassungsrechtlich nicht geboten sind.[55]

Das BVerfG hat in der Bestandsdatenauskunft I-Entscheidung erstmals das sogenannte Prinzip der Doppeltür ausführlich erläutert. Danach müssen die – jeweils zuständigen – Gesetzgeber nicht nur die Tür zur Übermittlung der Daten öffnen, sondern auch die Tür zu deren Abfrage.[56] Insoweit müsse schon der Gesetzgeber der Übermittlungsregelung in eigener Regelungsverantwortung eine klare und abschließende Entscheidung treffen, zu welchen Zwecken und mit welchen Begrenzungen er die erste Tür öffnet.[57]

Die hier besprochene Entscheidung enthält einige, teilweise dem Schrifttum entnommenen, Ergänzungen und Konkretisierungen dieses Prinzips. Es stellt beispielsweise klar, dass die erste Tür auch der Gesetzgeber der zweiten Tür nicht weiter öffnen könne. Er sei vielmehr insoweit an die in der Übermittlungsregelung getroffenen Verwendungsregeln gebunden. Dabei stehe es dem Gesetzgeber der Abrufregelungen zwar frei, den Datenabruf durch die berechtigten Behörden an noch engere Zwecke, höhere Eingriffsschwellen oder an den Schutz oder die Bewehrung noch gewichtigerer Rechtsgüter zu binden.[58]

Aus Gründen der Normenklarheit dürfe er aber selbst dann, wenn er – wie vorliegend – zugleich Gesetzgeber der Abrufregelungen ist, nicht die in der Übermittlungsregelung begrenzten Verwendungszwecke unterlaufen und die Behörden zum Abruf zu anderen, weitergehenden Zwecken ermächtigen, niedrigere Eingriffsschwellen oder einen weniger gewichtigen Rechtsgüterschutz vorsehen. Abrufregelungen mit solchermaßen abgesenkten Verwendungsregeln könnten zwar die Behörden – im Rahmen des verfassungsrechtlich Zulässigen – zum Datenabruf ermächtigen; die Diensteanbieter wären jedoch zur Auskunft weder berechtigt noch verpflichtet. Derartige Abrufregelungen enthielten von daher einen mit der Übermittlungsregelung von vornherein unvereinbaren Normbefehl. Die Verwendungszwecke der auszutauschenden Daten müssten aber gerade durch das Zusammenwirken der Übermittlungs- und Abrufregelung normenklar begrenzt sein. Es dürfe nicht der Anschein erweckt werden, dass eine Behörde losgelöst von den in der Übermittlungsregelung getroffenen Verwendungsregeln auf Daten zugreifen dürfte. Dadurch würden Zugriffsmöglichkeiten eröffnet, die missbräuchlich und unvorhersehbar ge-

46 Bestandsdatenauskunft II, Rn. 146.
47 Bestandsdatenauskunft II, Rn. 153.
48 Bestandsdatenauskunft II, Rn. 203.
49 Bestandsdatenauskunft II, Rn. 248 f.
50 Bestandsdatenauskunft II, Rn. 250.
51 Bestandsdatenauskunft II, Rn. 247 f.
52 Bestandsdatenauskunft II, Rn. 252 f.
53 Bestandsdatenauskunft II, Rn. 258 f.
54 Beschluss des ersten Senates vom 10.11.2020, 1 BvR 3214/15, Rn. 89.
55 Bestandsdatenauskunft II, Rn. 198.
56 Bestandsdatenauskunft I, Rn. 123.
57 BVerfGE 125, 260, Rn. 233.
58 Bestandsdatenauskunft II, Rn. 201 m.w.N.

nutzt werden könnten. Ein Widerspruch zwischen Übermittlungsregelung und einer weniger begrenzten Abrufregelung könnte auch nicht dahin aufgelöst werden, dass ein Datenaustausch nur unter den engeren Voraussetzungen der Übermittlungsregelung erfolgen dürfte. Die Einhaltung dieser engeren Voraussetzungen könnten und dürften die Diensteanbieter in materieller Hinsicht nicht überprüfen. Sie liege vielmehr allein in der Verantwortung der abfrageberechtigten Stellen und könne auch nur dort zuverlässig beurteilt werden. Sie würden aber durch die fachrechtlichen Abrufregelungen zu einem weitergehenden Datenabruf ermächtigt, ohne dass eine behördeninterne Kontrolle am Maßstab der Übermittlungsregelung gewährleistet wäre. Auch insoweit würden Zugriffsmöglichkeiten eröffnet, die rechtsstaatlich nicht mehr eingehegt und vorhersehbar wären.[59]

III. Darstellung der Entscheidungen in der Sache

Die Entscheidung erklärt die in Folge der Bestandsdatenauskunft I-Entscheidung des BVerfG geänderte Vorschrift des § 113 TKG (unten III. 1.) sowie die für verschiedene Sicherheitsbehörden neu geschaffenen Regelungen zum (manuellen) Abruf von Bestandsdaten (unten III. 2.) für in wesentlichen Teilen mit der Verfassung unvereinbar.

1. § 113 TKG

a) manuelle Bestandsdatenauskunft

In der Bestandsdatenauskunft I-Entscheidung hatte das Gericht festgestellt, dass die bisherige Vorschrift zur manuellen Abfrage von Bestandsdaten in verfassungskonformer Auslegung noch mit dem Grundgesetz vereinbar war.[60] Es hat dabei deutlich gemacht, dass es seine Entscheidung insbesondere auf die Tatsache gestützt hat, dass nach der geprüften Vorschrift Abfragen nur im Einzelfall zulässig waren und dies auch nur dann, wenn sie hierfür erforderlich waren. Dies sei zwar eine niedrige, jedoch noch ausreichende Eingriffsschwelle für derartige Eingriffe. Mittels verfassungskonformer Auslegung sei dabei immerhin sichergestellt, dass im Gefahrenabwehrbereich mindestens eine konkrete Gefahr und im Bereich der Strafverfolgung mindestens ein Anfangsverdacht erforderlich sei. Auskünfte „ins Blaue hinein" seien danach nicht möglich gewesen.[61] Umso unverständlicher war es, dass der Bundesgesetzgeber trotz dieser eindeutigen Formulierung in der auf die Entscheidung folgenden Neuregelung des § 113 TKG auch diese für verfassungskonform erklärte Regelung der manuellen Bestandsdatenauskunft angepasst und dabei das vom Gericht für bedeutsam erachtete Kriterium der Erforderlichkeit weggelassen hat. Folgerichtig und sozusagen mit Ankündigung hat das BVerfG in der vorliegend zu besprechenden Entscheidung dann auch diese Neuregelung zur manuellen Bestandsdatenauskunft für mit dem Grundgesetz unvereinbar erklärt. Es mangele an einer hinreichenden Eingriffsschwelle, um Abfragen „ins Blaue hinein" zu verhindern. Vielmehr bedürfe es in jedem Fall eines auf tatsächliche Anhaltspunkte gestützten Eingriffsanlasses. Unzulässig sei die Schaffung eines offenen Datenvorrats für vielfältige und ohne äußeren Eingriffsanlass begrenzte Verwendungen im gesamten einer Behörde zugewiesenen Aufgabenbereich.[62] Ausdrücklich wurde verneint, dass auch die vorliegende Regelung im Wege der Auslegung „geheilt" werden könne.[63]

Soweit eine entsprechende Eingriffsschwelle geregelt sei, seien darüber hinaus gehende Anforderungen an den Rechtsgüterschutz aufgrund des geringen Eingriffsgewichts grundsätzlich nicht erforderlich. Etwas anderes gelte jedoch dann, wenn anstatt einer konkreten Gefahr lediglich eine konkretisierte Gefahr[64] für die Anwendung der Maßnahme gefordert sei. Dann müsse die Absenkung der Eingriffsschwelle durch erhöhte Anforderungen an den Rechtsgüterschutz ausgeglichen werden. Unter diesen Voraussetzungen sei die Maßnahme nur zum Schutz von Rechtsgütern von zumindest erheblichem Gewicht zulässig.[65]

b) Auskünfte über Zugangssicherungscodes

In Leitsatz 5 der Bestandsdatenauskunft I-Entscheidung hatte das Gericht festgestellt, dass Auskünfte über Zugangssicherungscodes nur dann angefordert werden dürfen, wenn auch die gesetzlichen Voraussetzungen für ihre Nutzung gegeben sind. Es sei kein Grund ersichtlich, warum die Behörden die Zugangscodes unabhängig von den Anforderungen an deren Nutzung und damit gegebenenfalls unter leichteren Voraussetzungen abfragen können sollten.[66] Gleichwohl hat der Gesetzgeber in der Folge dieser Entscheidung zwar den Wortlaut des § 113 Abs. 1 Satz 2 TKG modifiziert. Inhaltlich entspricht die Regelung jedoch der Vorgängernorm.[67] Folgerichtig erklärt das Gericht somit auch die Neuregelung für verfassungswidrig und begründet dies in seltener Deutlichkeit: „Die Erklärung der Verfassungswidrigkeit einer Norm hindert den Gesetzgeber zwar nicht daran, eine inhaltlich gleichlautende Bestimmung wiederum zu erlassen (vgl. BVerfGE 77, 84 <103 f.>). Dabei kann er aber die vom Bundesverfassungsgericht festgestellten Gründe der Verfassungswidrigkeit des ursprünglichen Gesetzes nicht übergehen. Eine Normwiederholung verlangt vielmehr ihrerseits besondere Gründe, die sich vor allem aus einer wesentlichen Änderung der für die verfassungsrechtliche Beurteilung maßgeblichen tatsächlichen oder rechtlichen Verhältnisse oder der ihr zugrundeliegenden Anschauungen ergeben können. Fehlen solche Gründe, ist das Bundesverfassungsgericht nicht gehalten, die bereits entschiedenen verfassungsrechtlichen Fragen erneut zu erörtern (BVerfGE 96, 260 <263>). Solche Gründe sind hier nicht ersichtlich. […]".[68]

59 Vgl. im Ganzen: Bestandsdatenauskunft II, Rn. 201 f; Dazu auch Petri, ZD 2020, 580, 588 f.

60 Bestandsdatenauskunft I, Leitsatz 4.

61 Vgl. im Ganzen Bestandsdatenauskunft I, Rn. 177 f.

62 Vgl. insgesamt Bestandsdatenauskunft II, Leitsatz 4 und Rn. 145 und 154 f.

63 Bestandsdatenauskunft II, Rn. 156 f.

64 Vgl. oben I. d).

65 Bestandsdatenauskunft II, Rn. 150.

66 Bestandsdatenauskunft I, Rn. 184 f.

67 Bestandsdatenauskunft II, Rn. 160.

68 Bestandsdatenauskunft II, Rn. 161 f.

c) Zuordnung dynamischer IP-Adressen

Das BVerfG hatte in der Bestandsdatenauskunft I-Entscheidung festgestellt, dass eine Zuordnung dynamischer IP-Adressen nur unter gegenüber der manuellen Bestandsdatenauskunft gesteigerten Voraussetzungen verfassungsrechtlich zulässig sei. Dies hänge insbesondere damit zusammen, dass mit dieser Maßnahme nicht lediglich in das Recht auf informationelle Selbstbestimmung, sondern vielmehr in das Telekommunikationsgeheiminis aus Art. 10 GG eingegriffen würde.[69] Grund hierfür sei, dass die Telekommunikationsanbieter für die Identifizierung einer IP-Adresse in einem Zwischenschritt die entsprechenden Verbindungsdaten ihrer Kunden sichten müssten, also auf konkrete Telekommunikationsvorgänge (= Verkehrsdaten) zugreifen würden.[70] Die bisherige Regelung zur manuellen Bestandsdatenauskunft stellte somit keine verfassungskonforme Rechtsgrundlage für eine Abfrage dar, die eine Zuordnung dynamischer IP-Adressen erfordert.[71] Da die Sicherheitsbehörden nach dem Willen des Bundesgesetzgebers jedoch auch zu solchen Abfragen befugt sein sollen, war eine spezielle Rechtsgrundlage erforderlich. Diese wurde mit § 113 Abs. 1 Satz 3 TKG geschaffen. Danach durften die in eine manuelle Bestandsdatenauskunft „aufzunehmenden Daten auch anhand einer zu einem bestimmten Zeitpunkt zugewiesenen Internetprotokoll-Adresse bestimmt werden". Verkehrsdaten durften hierfür „auch automatisiert ausgewertet werden". In der hier zu besprechenden Entscheidung erklärte das BVerfG jedoch auch diese Norm für nicht mit dem Grundgesetz vereinbar.[72] Das Gericht bestätigte zunächst das gegenüber der manuellen Bestandsdatenauskunft erheblich erhöhte Eingriffsgewicht der Maßnahme.[73] Dieses mache näher begrenzende Eingriffsschwellen und teilweise erhöhte Anforderungen an den Rechtsgüterschutz erforderlich.[74] Als Eingriffsschwelle müsse grundsätzlich mindestens eine konkrete Gefahr bzw. ein Anfangsverdacht vorliegen.[75] Da bereits die manuelle Bestandsdatenauskunft nach § 113 Abs. 1 S. 1 TKG, auf die sich die Regelung bezieht, gegenüber der Vorgängerregelung keine hinreichenden Eingriffsschwellen (mehr) vorsah,[76] setzte sich dieser Mangel bei der Abfragemöglichkeit nach § 113 Abs. 1 S. 3 TKG fort. Die angegriffene Regelung war daher alleine aus diesem Grund bereits im Hinblick auf alle denkbaren Empfänger unverhältnismäßig.[77]

Abfragen von IP-Adressen seien aufgrund des gesteigerten Eingriffsgewichts zudem nur unter erhöhten Anforderungen an den Rechtsgüterschutz zulässig. Sie müssten mindestens dem Schutz oder der Bewehrung von Rechtsgütern von hervorgehobenem Gewicht dienen.[78] Hierzu gehörten jedenfalls die durch das Strafrecht geschützten Rechtsgüter.[79] Auch im Einzelfall besonders gewichtige Ordnungswidrigkeiten könnten hierunter fallen, wenn der Gesetzgeber sie ausdrücklich benenne.[80] Im Bereich der Gefahrenabwehr genüge jedenfalls nicht jede Gefahr für ein Schutzgut.[81] Für den Bereich der Nachrichtendienste müsse eine derartige Begrenzung der Rechtsgüter hingegen nicht ausdrücklich angeordnet werden, da deren Tätigkeit von vornherein dem Schutz besonders gewichtiger Rechtsgüter in diesem Sinne diene.[82] Da die angegriffene Regelung keine Anforderungen an den Rechtsgüterschutz enthielt, war sie somit neben der fehlenden Eingriffsschwelle im Hinblick auf alle Empfänger außer den Nachrichtendiensten zusätzlich auch aus diesem Grund unverhältnismäßig.[83]

Sofern die Abfrage von IP-Adressen über die reguläre Eingriffsschwelle der konkreten Gefahr hinaus auch schon bei einer lediglich konkretisierten Gefahr zulässig sein soll, sei die damit verbundene Absenkung der Eingriffsschwelle durch eine weitere Erhöhung der Anforderungen an den Rechtsgüterschutz auszugleichen. Statt dem Schutz von Rechtsgütern von mindestens hervorgehobenem Gewicht sei die Abfrage dann nur zum Schutz von besonders gewichtigen Rechtsgütern verhältnismäßig.[84] Soweit die Gefahrenabwehr der Verhütung von Straftaten diene, müssten mindestens schwere Straftaten verhindert werden.[85]

Darüber hinaus bedürfe es insgesamt der gesetzlichen Regelung einer nachvollziehbaren und überprüfbaren Dokumentation der Entscheidungsgrundlagen für die Anfrage.[86]

2. Die Abrufregelungen der Sicherheitsbehörden

Die mit der Verfassungsbeschwerde angegriffenen Abrufregelungen der Sicherheitsbehörden sind sich weitgehend ähnlich. Sie werden daher im Folgenden zusammenfassend behandelt, soweit nicht Unterschiede eine differenzierende Betrachtung erforderlich machen.

Entsprechend den für die Öffnung der Datenbestände entwickelten Maßstäben,[87] müssen auch die Abrufregelungen ihrerseits die Verwendungszwecke der Daten hinreichend begrenzen. Dabei sind Anlass, Zweck und Umfang des jeweiligen Eingriffs auch für den Datenabruf bereichsspezifisch, präzise und normenklar festzulegen. Zudem sind auch für den Abruf Eingriffsschwellen erforderlich, die sicherstellen, dass Auskünfte nur bei einem auf tatsächliche Anhaltspunkte gestützten Eingriffsanlass eingeholt werden können. Unzulässig ist der Abruf für vielfältige und unbegrenzte Verwendungen im gesamten einer Behörde zugewiesenen Aufgabenbereich.[88]

69 Bestandsdatenauskunft I, Rn. 109 f.
70 Bestandsdatenauskunft I, Rn. 116 und Bestandsdatenauskunft II, Rn. 99 f.
71 Bestandsdatenauskunft I, Rn. 164.
72 Bestandsdatenauskunft II, Leitsatz 4.
73 Bestandsdatenauskunft II, Rn. 165 f.
74 Bestandsdatenauskunft II, Rn. 175 f.
75 Bestandsdatenauskunft II, Rn. 176.
76 Vgl. oben III. 1. a).
77 Bestandsdatenauskunft II, Rn. 183 f.
78 Bestandsdatenauskunft II, Rn. 178.
79 Bestandsdatenauskunft II, Rn. 178.
80 Bestandsdatenauskunft II, Rn. 177 und 178.
81 Bestandsdatenauskunft II, Rn. 177.
82 Bestandsdatenauskunft II, Rn. 182.
83 Bestandsdatenauskunft II, Rn. 185 und 186.
84 Bestandsdatenauskunft II, Rn. 180.
85 Bestandsdatenauskunft II, Rn. 181.
86 Bestandsdatenauskunft II, Rn. 244.
87 Vgl. oben III. 1. a)
88 Bestandsdatenauskunft II, Rn. 197.

a) manuelle Bestandsdatenauskünfte

Die allgemein zum Abruf von Bestandsdaten ermächtigenden § 10 Abs. 1 Satz 1, 2 und 3 BKAG, § 7 Abs. 5 Satz 1, § 15 Abs. 2 Satz 1 ZFdG, § 8d Abs. 1 Satz 1 BVerfSchG sowie § 2b Satz 1 BNDG und § 4b Satz 1 MADG, soweit sie auf § 8d Abs. 1 Satz 1 BVerfSchG verweisen, seien hinsichtlich ihrer Eingriffsschwellen nicht hinreichend eingegrenzt und daher unverhältnismäßig.[89] Eine Erforderlichkeit der Auskunft lediglich zur Erfüllung einer der jeweiligen Behörde obliegenden Aufgabe stelle keine hinreichend begrenzte Eingriffsschwelle dar.[90] Dies gelte selbst dann, wenn die Bestandsdaten nur zur Ergänzung vorhandener Sachverhalte oder sonst zu Zwecken der Auswertung erhoben werden dürfen, da diese Einschränkung am Vorfeldcharakter einer solchen Abfragemöglichkeit nichts ändere.[91] Vielmehr müsse sich das Erfordernis einer Gefahr oder eines Anfangsverdachts aus dem Gesetzestext selbst ergeben.[92] Soweit das BKA zu Bestandsdatenauskünften auf dem Gebiet der Strafverfolgung ermächtigt wurde, kam § 10 Abs. 1 S. 1 BKAG nach den Feststellungen des Gerichts von vornherein nicht als Ermächtigungsgrundlage in Betracht. Da als Eingriffsschwelle mindestens ein Anfangsverdacht erforderlich sei, gelte ab diesem Zeitpunkt die StPO mit den dort geregelten Ermächtigungsgrundlagen und ende die Zuständigkeit des BKAG nach § 2 Abs. 2 Nr. 2 BKAG.[93] Gleiches gelte für die Zollkriminalämter, soweit ihnen die Aufdeckung unbekannter Straftaten und die Vorsorge für künftige Strafverfahren als jeweils repressivpolizeiliche Aufgaben obliege bzw. sie bei der Bekämpfung der international organisierten Geldwäsche mitwirkten und insoweit originär strafverfolgend tätig würden.[94] Differenzierter sei dagegen § 40 Abs. 1 Satz 1 BKAG zu betrachten. Soweit § 40 Abs. 1 Satz 1 BKAG auf § 39 Abs. 1 und Abs. 2 Nr. 1 BKAG Bezug nimmt, sei die Maßnahme mangels hinreichender Eingriffsschwellen verfassungswidrig.[95] Keinen verfassungsrechtlichen Bedenken unterliege demgegenüber § 40 Abs. 1 Satz 1 BKAG, soweit er auf § 39 Abs. 2 Nr. 2 BKAG Bezug nimmt. Insoweit seien ausreichende Eingriffsschwellen und hinreichende Anforderungen an den Rechtsgüterschutz geregelt.[96] Gleiches gelte für § 22a Abs. 1 Satz 1 BPolG. Soweit er auf § 21 Abs. 1 und auf § 21 Abs. 2 Nr. 1 BPolG verweist, fehlten hinreichende Eingriffsschwellen. Soweit ein Verweis auf § 21 Abs. 2 Nr. 2 BPolG erfolge, sei die Maßnahme jedoch verfassungskonform ausgestaltet.[97]

b) Auskünfte über Zugangssicherungscodes

Die im Rahmen der hier zu besprechenden Entscheidung relevanten Abrufvorschriften zu Zugangssicherungscodes wurden sämtlich gemäß den Vorgaben des Gerichts aus der Bestandsdatenauskunft I-Entscheidung[98] verfasst und daher auch nunmehr für verfassungskonform erachtet.[99] Insbesondere bedürfe es keiner ergänzenden Subsidiaritätsklausel, wonach eine Abfrage nur dann erfolgen darf, wenn die damit bezweckte Datenerhebung nicht auf andere Weise erreicht werden kann.[100] Zudem sei es von Verfassung wegen auch unbeachtlich, dass es für den Abruf von Zugangsdaten nach § 10 Abs. 1 Satz 1 Nr. 1, Satz 2 BKAG und § 7 Abs. 5 Satz 2 ZFdG keinen praktischen Anwendungsbereich gebe, weil weder das BKA noch das ZKA über entsprechende Befugnisse verfügen würden.[101]

c) Auskünfte zu IP-Adressen

Die angegriffenen Regelungen zum Abruf von Bestandsdaten, die anhand einer dynamischen IP-Adresse bestimmt werden (§ 10 Abs. 2, § 40 Abs. 2 BKAG, § 22a Abs. 2 BPolG, § 7 Abs. 6, § 15 Abs. 3 ZFdG, § 8d Abs. 2 Satz 1 BVerfSchG sowie § 2b Satz 1 BNDG und § 4b Satz 1 MADG, soweit sie auf § 8d Abs. 2 Satz 1 BVerfSchG verweisen), sind ganz überwiegend nicht hinreichend eingegrenzt und schon deshalb unverhältnismäßig.[102] Dabei seien im Vergleich zur manuellen Bestandsdatenauskunft zwar keine erhöhten Eingriffsschwellen erforderlich. Wie bei der Komplementärvorschrift des § 113 Abs. 1 TKG[103] setze sich jedoch auch bei den Abrufregelungen in § 10 Abs. 2 BKAG, § 40 Abs. 2 in Verbindung mit § 39 Abs. 1 und 2 Nr. 1 BKAG, § 22a Abs. 2 in Verbindung mit § 21 Abs. 1 und 2 Nr. 1 BPolG, § 7 Abs. 6 und § 15 Abs. 3 ZFdG, § 8d Abs. 2 Satz 1 BVerfSchG sowie § 2b Satz 1 BNDG und § 4b Satz 1 MADG, soweit sie auf § 8d Abs. 2 Satz 1 BVerfSchG verweisen, die bereits für die manuelle Bestandsdatenauskunft fehlende Regelung hinreichender Eingriffsschwellen fort.[104]

Aufgrund des erhöhten Eingriffsgewichts bedürfe es zudem – wie auch bei der Übermittlungsvorschrift nach § 113 Abs. 1 Satz 3 TKG[105] – ausdrücklich geregelter erhöhter Anforderungen an den Rechtsgüterschutz.[106] Jedoch gelte auch hier eine Ausnahme für die Nachrichtendienste.[107] Da deren in Bezug genommenen Aufgaben durchweg dem Schutz besonders gewichtiger Rechtsgüter dienen, wäre im Hinblick auf das Eingriffsgewicht diesbezüglich sogar eine lediglich konkretisierte Gefahr als Eingriffsschwelle ausreichend.[108] Die übrigen Vorschriften würden jedoch auch den Verhältnismäßigkeitsanforderungen hinsichtlich der Anforderungen an den Rechtsgüterschutz weitgehend nicht gerecht.[109] Zwar erforderten § 10 Abs. 2, Abs. 1 N. 1 BKAG und § 22a Abs. 2 i.V.m. § 21 Abs. 2 BPolG

89 Bestandsdatenauskunft II, Rn. 189 f.
90 Vgl. oben III. 1. a).
91 Bestandsdatenauskunft II, Rn. 210.
92 Bestandsdatenauskunft II, Rn. 213.
93 Bestandsdatenauskunft II, Rn. 212.
94 Bestandsdatenauskunft II, Rn. 216.
95 Bestandsdatenauskunft II, Rn. 219 f.
96 Bestandsdatenauskunft II, Rn. 227 f.
97 Bestandsdatenauskunft II, Rn. 229 f.
98 Vgl. oben III. 1. b).
99 Bestandsdatenauskunft II, Rn. 234.
100 Bestandsdatenauskunft II, Rn. 192.
101 Bestandsdatenauskunft II, Rn. 236.
102 Bestandsdatenauskunft II, Rn. 237.
103 Vgl. oben III. 1. c).
104 Bestandsdatenauskunft II, Rn. 239.
105 Vgl. oben III. 1. c).
106 Bestandsdatenauskunft II, Rn. 238.
107 Vgl. oben III. 1. c).
108 Bestandsdatenauskunft II, Rn. 240.
109 Bestandsdatenauskunft II, Rn. 242.

eine differenzierte Betrachtung. Im Ergebnis stellten jedoch auch sie nicht ausreichend hohe Anforderungen an den Rechtsgüterschutz.[110]

Allein § 40 Abs. 2 BKAG genüge, soweit er auf § 39 Abs. 2 Nr. 2 BKAG Bezug nimmt, insoweit den Verhältnismäßigkeitsanforderungen.[111] Jedoch werden die ergänzend erforderlichen verfahrensrechtlichen Anforderungen nicht erfüllt.[112]

IV. Fazit und Ausblick

Nach Graulich wurden in den beiden Entscheidungen zum BKAG und der Bestandsdatenauskunft I die Grundrechte als Stimmgabeln an den einfachgesetzlichen Normen zum Schwingen gebracht und auf ihre Stimmigkeit abgehört.[113] Um im musikalischen Bild zu bleiben, gibt die vorliegende Entscheidung in Abhängigkeit der nach dem Gesetzgeber zu spielenden Melodie und deren Tonlage vor, mit welchen Instrumenten die Melodie zu spielen ist und wie stark deren Saiten anzuschlagen sind. Dabei stellt sich das Kriterium der Anforderungen an den Rechtsgüterschutz als das zentrale Instrument der Verhältnismäßigkeit heraus, dessen Saitenanschlag maßgeblich über den verfassungsmäßigen Wohlklang der gespielten Melodie entscheidet.

Nach der Bestandsdatenauskunft II-Entscheidung des Gerichts hat der Gesetzgeber eine Regelungsfrist bis zum 31.12.2021. Diese scheint er jedoch nicht auszuschöpfen. Bereits im Dezember 2020 wurde ein „Entwurf für ein Gesetz zur Anpassung der Regelungen über die Bestandsdatenauskunft an die Vorgaben aus der Entscheidung des Bundesverfassungsgerichts vom 27.05.2020"[114] in den Bundestag eingebracht, der bereits im Januar 2021 verabschiedet wurde. Mit der zügigen Korrektur[115] kommt der Gesetzgeber zwar der Empfehlung der Datenschutzkonferenz (DSK) nach, die vom Gericht gesetzte Frist nicht auszureizen.[116] Hintergrund der zügigen Neuregelung sind jedoch mutmaßlich weniger die Mahnungen der DSK. Vielmehr hat die BVerfG-Entscheidung das Inkrafttreten zweier bereits verabschiedeter Gesetzentwürfe[117] verzögert, die gleichlautende Abrufregelungen enthielten, wie sie das Gericht in der vorliegenden Entscheidung für verfassungswidrig befunden hat. Die Gesetzentwürfe waren in der Folge nicht vom Bundespräsidenten ausgefertigt worden. Der Gesetzentwurf zur Änderung der Bestandsdatenauskünfte umfasst 58 Seiten und sieht neben der Korrektur von Bestandsdatenauskünften hinsichtlich Telekommunikationsvorgängen auch die Erweiterung auf Telemedien vor. Diese über die reine Umsetzung der hier besprochenen Entscheidung erneut hinausgehende Erweiterung der Eingriffsbefugnisse birgt abermals das Risiko, zumindest in Teilen verfassungswidrig zu sein. Es ist daher mit Spannung zu erwarten, ob der Gesetzgeber dieses Mal die von ihm gewünschte Melodie und Tonlage mit den nach dem BVerfG erforderlichen Instrumenten und einem ausgewogenen Saitenanschlag spielt. Einige Sachverständige haben hieran Zweifel angemeldet.[118] Der Entwurf wurde daraufhin gleichwohl kaum angepasst.[119] Die Zuhörerschaft darf somit gespannt sein, ob das BVerfG ein drittes Mal um Prüfung ersucht wird und wie für diesen Fall seine Entscheidung ausfallen wird.

Sebastian Lottkus
Referent im Bereich öffentliche Stellen (insbesondere Polizei, Staatsanwaltschaften und Verfassungsschutz) bei der Landesbeauftragten für Datenschutz und Informationsfreiheit Nordrhein-Westfalen

110 Bestandsdatenauskunft II, Rn. 241.

111 Bestandsdatenauskunft II, Rn. 237.

112 Bestandsdatenauskunft II, Rn. 248 f.

113 Graulich, Polizeiliche Gefahrenabwehr mit heimlichen Überwachungsmaßnahmen – Anm. zu BVerfG, Urt. v. 20.04.2016 – 1 BvR 966/09, 1 BvR 1140/09 – zum BKAG, KriPoZ 2016, 75.

114 BT-Drucksache 19/25294.

115 Im Gesetzgebungsverfahren wurde der Begriff „Reparaturgesetz" geprägt – vgl. nur Plenarprotokoll 19/206, S. 25992 (A) und (C).

116 Entschließung der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder vom 25.11.2020 – „Auskunftsverfahren für Sicherheitsbehörden und Nachrichtendienste verfassungskonform ausgestalten".

117 Gesetz zur Neustrukturierung des Zollfahndungsdienstgesetzes (ursprünglicher Entwurf BT-Drucksache 19/12088) und Gesetz zur Bekämpfung des Rechtsextremismus und der Hasskriminalität (ursprünglicher Entwurf BT-Drucksache 19/17741).

118 Vgl. Bäcker, Stellungnahme zu dem Entwurf eines Gesetzes zur Anpassung der Regelungen über die Bestandsdatenauskunft an die Vorgaben aus der Entscheidung des Bundesverfassungsgerichts vom 27.05.2020 (BT-Drs. 19/25294) – Ausschussdrucksache 19(4)696 A; Löffelmann, Schriftliche Stellungnahme zur öffentlichen Anhörung am 25. Januar 2021 zu BT-Drs. 19/25294, Ausschussdrucksache 19(4)696 B; der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit, Stellungnahme des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit für die öffentliche Anhörung des Ausschusses für Inneres und Heimat des Deutschen Bundestages am 25.01.2021 zum Entwurf eines Gesetzes zur Anpassung der Regelungen über die Bestandsdatenauskunft an die Vorgaben aus der Entscheidung des Bundesverfassungsgerichts vom 27.05.2020 (BT-Drucksache 19/25294), Ausschussdrucksache 19(4)696 D.

119 BT-Drucksache 19-26267, S. 4.

Kurzbeiträge

Zur strafrechtlichen Neubewertung der Verkehrsdatenspeicherung[1]

Peter Biesenbach/Markus Hartmann*

Über die sogenannte Vorratsdatenspeicherung, besser und genauer: Verkehrsdatenspeicherung, ist sowohl justiz- als auch gesellschaftspolitisch viel gestritten und gerungen worden. Schon der Begriff selbst ist alles andere als trennscharf. Das geltende Recht wird derzeit weitgehend nicht umgesetzt. Die Folgen für die Strafrechtspraxis sind erheblich. Nachdem der Europäische Gerichtshof jüngst den (europa-) rechtlichen Handlungsrahmen deutlicher konturiert hat, ist es an der Zeit, die nationale Rechtslage hin zu einer begrenzten IP-Zuordnung zu schärfen.

I. Kurzüberblick über die aktuelle Rechtslage; Bedeutung für die strafrechtliche Praxis

Die Verkehrsdatenspeicherung ist in den § § 113a ff. TKG gesetzlich geregelt. Verpflichtet sind „Erbringer öffentlich zugänglicher Telekommunikationsdienste für Endnutzer" (§ 113a Abs. 1 Satz 1 TKG), d.h. insbesondere Internetzugangsprovider und Anbieter von Telefondiensten. Die Speicherpflicht erstreckt sich auf ausgewählte Verkehrsdaten (§ 113b Abs. 2 und 3 TKG) für zehn Wochen (§ 113b Abs. 1 TKG) und – im Fall der Mobilfunkkommunikation – auf Standortdaten (§ 113b Abs. 4 TKG) für vier Wochen (§ 113b Abs. 1 TKG).

Der Zugang zu den gespeicherten Daten ist nach dem „Doppeltürmodell"[2] des Bundesverfassungsgerichts ausgestaltet. Während § 113c TKG die Datenübermittlungsbefugnis der Telekommunikationsanbieter normiert, ist der Zugriff der Strafverfolgungsbehörden in § 100g Abs. 2 StPO geregelt. Dieser sieht in Satz 2 einen Katalog besonders schwerer Straftaten vor, bei denen der Zugriff auf gespeicherte Daten legitimiert ist, sofern die Tat auch im Einzelfall besonders schwer wiegt und die Erforschung des Sachverhalts oder die Ermittlung des Aufenthaltsortes des Beschuldigten auf andere Weise wesentlich erschwert oder aussichtslos wäre und die Erhebung der Daten in einem angemessenen Verhältnis zur Bedeutung der Sache steht.

Die Verkehrsdatenspeicherung wird von der Bundesnetzagentur gegenüber den Telekommunikationsprovidern derzeit infolge eines Beschlusses des Oberverwaltungsgerichts Nordrhein-Westfalen vom 22.06.2017 (13 B 238/17) nicht durchgesetzt. Das Oberverwaltungsgericht hatte insoweit festgestellt, dass die im Dezember 2015 gesetzlich eingeführte und ab dem 1. Juli 2017 wirksame Pflicht für die Erbringer öffentlich zugänglicher Telekommunikationsdienste zur Speicherung von bei der Nutzung von Telefon- und Internetdiensten anfallenden Verkehrs- und Standortdaten ihrer Nutzer mit dem Recht der Europäischen Union nicht vereinbar sei.[3]

Daher sieht die Bundesnetzagentur seitdem und bis zum rechtskräftigen Abschluss eines Hauptsacheverfahrens von Anordnungen und sonstigen Maßnahmen zur Durchsetzung der in § 113b TKG geregelten Speicherverpflichtungen gegenüber allen verpflichteten Unternehmen ab.[4] Bußgeldverfahren werden wegen Verletzung der Speicherverpflichtungen nicht eingeleitet.

Den Strafverfolgungsbehörden stehen im Ergebnis der vorbezeichneten Rechts- und Rechtsdurchsetzungssituation Verkehrs- und Standortdaten derzeit regelmäßig nur zur Verfügung, soweit die Telekommunikationsanbieter diese für ihre internen technischen Prozesse und die Netzsicherheit vorhalten dürfen. Dieser Zeitraum erstreckt sich im Regelfall auf nicht mehr als sieben Kalendertage. Soweit eine öffentlich bekannt gewordene Erhebung der Bundesnetzagentur eine teils deutlich längere Speicherpraxis der Telekommunikationsanbieter ausweist,[5] kann nach den Erfahrungen der Praxis eine belastbar längere Speicherpraxis nicht festgestellt werden.

Die Auswirkungen des fehlenden Zugriffs auf Verkehrs- und Standortdaten sind für Erfolg und Effektivität der Strafverfolgung erheblich. Sie erstrecken sich entsprechend des Katalogs des § 100g Abs. 2 Satz 2 StPO auf fast alle Deliktsfelder besonders schwerer Kriminalität. In Nordrhein-Westfalen ist nach den mit den Stichworten „Lügde", „Bergisch Gladbach" und „Münster" verknüpften Tatkomplexen besonders der Bereich der Bekämpfung digitaler Abbildungen von Kindesmissbrauch und der Kindesmissbrauch in digitalen Medien selbst in den Fokus genommen worden. Hier ist regelmäßig insbesondere in Fällen von Hinweisen ausländischer Behörden und Organisationen eine Täteridentifikation nur dann möglich, wenn und solange über den Zugriff auf Daten der Telekom-

* Peter Biesenbach ist Minister der Justiz des Landes Nordrhein-Westfalen. Markus Hartmann ist Oberstaatsanwalt als Hauptabteilungsleiter, Leiter der Zentral- und Ansprechstelle Cybercrime Nordrhein-Westfalen (ZAC NRW).

1 Der Beitrag beschränkt sich auf den Bereich der Strafrechtspflege. Das Gefahrenabwehrrecht und das Recht der Nachrichtendienste bleiben außer Betracht.

2 Zu vgl. BVerfG, Beschluss des Ersten Senats vom 24. Januar 2012, 1 BvR 1299/05 (BVerfGE 130, 151).

3 Zu vgl. https://www.justiz.nrw.de/nrwe/ovgs/ovg_nrw/j2017/13_B_238_17_Beschluss_20170622.html.

4 Zu vgl. Mitteilung der Bundesnetzagentur, abzurufen unter https://www.bundesnetzagentur.de/DE/Sachgebiete/Telekommunikation/Unternehmen_Institutionen/Anbieterpflichten/OeffentlicheSicherheit/Umsetzung110TKG/VDS_113aTKG/VDS.html.

5 Zu vgl. http://www.Verkehrsdatenspeicherung.de/images/vb_breg_anl4_2018-05-15.pdf.

munikationsprovider IP-Adressen auf die tatsächlichen Anschlüsse oder Endgeräte aufgelöst werden können.

II. Europa- und verfassungsrechtlicher Handlungsrahmen; Bewertung

Unbeschadet dieser Zustandsbeschreibung der Ermittlungswirklichkeit ist bei nüchterner Betrachtung des verfassungs- und europarechtlichen Handlungsrahmens und der diesen konkretisierenden Rechtsprechung zu konstatieren, dass ein umfassender regulativer Ansatz, der terminologisch mit dem Begriff der Verkehrsdatenspeicherung verknüpft ist, rechtlich kaum umsetzbar sein dürfte. Die Verkehrsdatenspeicherung ist tot. Aus ihrem Nachlass sind jedoch die rechtlich tragfähigen und strafverfolgungspraktisch bedeutsamsten Regelungen zu identifizieren. Dies gelingt vor allem mit Blick auf die in den Entscheidungen des EuGH entwickelten Grundsätze.

1. Der EuGH hat sich in verschiedenen Entscheidungen mit der Verkehrsdatenspeicherung befasst und einen europarechtlich zulässigen Handlungsrahmen herausgearbeitet. Die Urteile des Gerichtshofs (Große Kammer) vom 08.04.2014 (Digital Rights Ireland Ltd gegen Minister for Communications, Marine and Natural Resources u.a. und Kärntner Landesregierung u.a., C-293/12 und C-594/12) und vom 21.12.2016 (Tele2 Sverige AB gegen Post- och telestyrelsen und Secretary of State for the Home Department gegen Tom Watson u.a., C-203/15 und C-698/15) kulminieren in dem Urteil vom 06.10.2020 (La Quadrature du Net u.a. gegen Premier ministre u.a., C-511/18, C-512/18, C-520/18), das erstmals neben der Bestätigung der grundsätzlichen Europarechtwidrigkeit einer allgemeinen Verkehrsdatenspeicherung rechtlich zulässige Anwendungsfälle herausarbeitet.

Demnach ist eine Verkehrsdatenspeicherung grundsätzlich unzulässig.[6] In einzeln erläuterten Ausnahmefällen kann eine begrenzte Datenspeicherung hingegen zulässig sein. Hierzu führt der Gerichtshof die folgenden Anwendungsfälle an:

a) Nationale Sicherheit

Sofern sich ein Mitgliedsstaat einer als real und aktuell oder vorhersehbar einzustufenden ernsten Bedrohung für die nationale Sicherheit gegenübersieht, soll eine allgemeine Verkehrsdatenspeicherung zulässig sein, wenn sie unter effektiven Rechtsgarantien und zeitlich auf das absolut Notwendige beschränkt erfolgt.

b) Räumlich oder in persönlicher Hinsicht begrenzte Datenspeicherung

Zum Schutz der nationalen Sicherheit, zur Bekämpfung schwerer Kriminalität und zur Verhütung schwerer Bedrohungen der öffentlichen Sicherheit ist die Verkehrsdatenspeicherung zulässig, wenn sie anhand von Kategorien betroffener Personen oder mittels eines geografischen Kriteriums begrenzt bleibt sowie die Speicherdauer eng eingrenzt wird.

c) Zuordnungsdaten von IP-Adressen

Für IP-Adressen konstatiert der Gerichtshof ein geringeres Schutzbedürfnis. Wenngleich er ausführt, IP-Adressen seien aussagekräftig betreffend das Online-Verhalten einer Person, wird ihre herausgehobene Bedeutung zur Identifikation einer Person im Internet anerkannt. Der Gerichtshof hebt insbesondere das Deliktsfeld der Kinderpornografie und des sexuellen Missbrauchs respektive der sexuellen Ausbeutung von Kindern insoweit hervor. Er geht davon aus, dass zum Schutz der nationalen Sicherheit, zur Bekämpfung schwerer Kriminalität und zur Verhütung schwerer Bedrohungen der öffentlichen Sicherheit eine zeitlich auf das absolut Notwendige begrenzte, indes generelle Speicherung der IP-Adressen, die der Quelle einer Verbindung zugewiesen sind, zulässig ist. Maßnahmen und Verfahrensgarantien zur Verhinderung eines Trackings des Online-Verhaltens von Personen sind geboten. Bloße Bestandsdaten können hingegen zeitlich unbegrenzt gespeichert bzw. genutzt werden.

d) Umgehende Sicherung von Verkehrs- und Standortdaten

Nach dem Urteil des Gerichtshofs kann nationales Recht Regelungen treffen, für die Bekämpfung schwerer Straftaten und zum Schutz der nationalen Sicherheit auf Verlangen der zuständigen Behörden Verkehrs- und Standortdaten durch die Provider im Einzelfall anlassbezogen fortdauernd speichern zu lassen. Hierzu bedarf es jedoch der Beschränkung auf einen ermittlungsrelevanten Personenkreis oder eine ermittlungsrelevante Geolokalisation.

2. Die durch den Gerichtshof gebildeten Fallgruppen lassen sich nur bedingt auf die strafrechtliche Ermittlungspraxis anwenden. Die Fallgruppe der nationalen Sicherheit dürfte nach den Vorgaben des Gerichts allenfalls auf den Bereich der Terrorabwehr und die nachrichtendienstliche Sphäre begrenzt relevant sein. Eine darüber hinausgehende nationale strafrechtliche Umsetzbarkeit ist nicht ersichtlich. Eine personell begrenzte Datenspeicherung für einen konkret benannten Personenkreis (etwa Gefährder und deren Kontaktpersonen) dürfte nach deutschem Strafprozessrecht eher Maßnahmen der Telekommunikationsüberwachung als einer Verkehrsdatenspeicherung entsprechen. Eine räumliche Begrenzung ist hingegen auch als eingegrenzte Datenspeicherung denkbar etwa für Verbrechensschwerpunkte oder besonders gefährdete Orte – der Gerichtshof nennt Flughäfen, Bahnhöfe oder Zollanlagen. „Umgehende Sicherung von Verkehrs- und Standortdaten" dürfte dem unter dem Begriff „Quick Freeze" diskutierten Regelungsmodell gleichkommen. Dieses stellt jedoch nur eine erleichterte Verhinderung der Datenlöschung, jedoch keine Datenspeicherung im eigentlichen Sinne dar. Ohne die zu „Quick Freeze" diskutierten Argumente im Detail zu beleuchten ist jedenfalls festzuhalten, dass diesem nur tat-

6 „Art. 15 Abs. 1 der Richtlinie 2002/58/EG des Europäischen Parlaments und des Rates vom 12.07.2002 über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation (Datenschutzrichtlinie für elektronische Kommunikation) in der durch die Richtlinie 2009/136/EG des Europäischen Parlaments und des Rates vom 25.11.2009 geänderten Fassung ist im Licht der Art. 7, 8 und 11 sowie von Art. 52 Abs. 1 der Charta der Grundrechte der Europäischen Union dahin auszulegen, dass er Rechtsvorschriften entgegensteht, die zu den in Art. 15 Abs. 1 genannten Zwecken präventiv eine allgemeine und unterschiedslose Vorratsspeicherung von Verkehrs- und Standortdaten vorsehen."

sächlich vorhandene Daten unterfallen können. Das Problem originär begrenzter Datenverfügbarkeit wird nicht gelöst. Insbesondere in Cybercrimefällen und Sachverhalten mit prägenden Online-Bezügen erweist sich „Quick Freeze" überdies wegen der regelmäßig relevanten Ketten computerforensischer Beweismittel als untauglich.

Damit verbleibt für einen strafprozessualen Gestaltungsraum derzeit allein die Fallgruppe der Speicherung von Zuordnungsdaten zu IP-Adressen.

Auch das Bundesverfassungsgericht geht von einer geringeren Schutzbedürftigkeit von Zuordnungsdaten zu IP-Adressen aus, betont allerdings auch die Bedeutung für die Erfassung des Online-Verhaltens von Personen.[7] Gleichwohl ließen sich „systematische Ausforschungen über einen längeren Zeitraum oder die Erstellung von Persönlichkeits- und Bewegungsprofilen (…) allein auf Grundlage solcher Auskünfte gerade nicht verwirklichen".[8] Mit Blick auf die Vorgaben des EuGH dürfte jedenfalls nationales Verfassungsrecht einer Neuregelung der Verkehrsdatenspeicherung unter dem (begrenzten) Aspekt der Speicherung von Zuordnungsdaten zu IP-Adressen nicht entgegenstehen.

III. Ausgestaltung des Handlungsspielraums im strafprozessualen Bereich

Eine Neuordnung der Verkehrsdatenspeicherung kann in strafrechtlicher Hinsicht derzeit nur unter dem Gesichtspunkt der Speicherung von Zuordnungsdaten zu IP-Adressen erfolgen. Sie wäre trotz des beschränkten Anwendungsbereichs aus Sicht der Strafrechtpraxis gleichwohl sinnvoll. Denn die mangelnde Fähigkeit, IP-Adressen auf physikalische Anschlüsse oder Endgeräte aufzulösen, erweist sich in einer Vielzahl von Ermittlungssituationen digitaler Kriminalität als wesentliches Verfahrenshemmnis. Namentlich der vom Europäischen Gerichtshof thematisierte Bereich der Bekämpfung digitaler Abbildungen von Kindesmissbrauch erfordert regelmäßig entsprechende Zuordnungen zur Identifizierung tatverdächtiger Personen. Sind die Daten länger als derzeit maximal sieben Tage für die Strafverfolgungsbehörden verfügbar, ist mit einer deutlichen Steigerung erfolgreicher Identifizierungen zu rechnen.

Unter Berücksichtigung der europa- und verfassungsrechtlichen Vorgaben sind folgende Eckpunkte im Bereich der Strafrechtspflege in den Blick zu nehmen:

1. Begrifflichkeit

Der Begriff der Verkehrsdatenspeicherung ist in der rechtspolitischen Diskussion belastet. Die Positionen scheinen in dogmatischen „Lagern" verhaftet zu sein. Die hier skizzierten Regelungsbereiche erfassen lediglich einen kleinen Teilbereich der bisherigen Rechts- und Diskussionslage, auf den der überkommene Begriff nicht sinngleich zutrifft. Die Bezeichnung „begrenzte IP-Zuordnung" trifft den Kern des Intendierten.

2. Zeitliche Begrenzung

Zur Wahrung der Verhältnismäßigkeit insbesondere unter dem Aspekt der Profilbildung bezüglich des Online-Verhaltens ist eine zeitliche Beschränkung der Datenspeicherdauer sachgerecht. Nach der bisherigen gesetzlichen Regelung ist die maximale Speicherfrist für Verkehrsdaten (ohne Standortdaten) auf 10 Wochen begrenzt. Mit Blick auf die Vorgaben des EuGH und die dort geforderte zeitliche Beschränkung auf das absolut Notwendige dürfte die geltende restriktive Regelung einen zulässigen Speicherzeitraum abbilden. Da der bisherige § 113b Abs. 1 Nr. 1 TKG die Zehnwochenfrist jedoch auf den grundrechtlich invasiveren Eingriff in alle Verkehrsdaten nach den Absätzen 2 und 3 der Norm erstreckt, könnte wegen der geringeren Schutzbedürftigkeit bloßer IP-Adressen auch eine moderat darüber hinausgehende Speicherung in Betracht zu ziehen sein, ohne dass Anlass zu der Besorgnis übermäßiger Datenhaltung respektive einer Überschreitung der Vorgaben des EuGH bestünde.

3. Zugriffsvoraussetzungen

Das Bundesverfassungsgericht hat in seinem Beschluss vom 27.05.2020 ausgeführt, „erforderlich" seien „grundsätzlich die Reichweite des § 113 Abs. 1 Satz 3 TKG näher begrenzende Eingriffsschwellen sowie eine Beschränkung auf den Schutz oder die Bewehrung von Rechtsgütern von hervorgehobenem Gewicht."[9] Voraussetzung in strafrechtlicher Hinsicht ist demnach der Anfangsverdacht einer Straftat. Mit Blick auf die restriktiveren Vorgaben des EuGH dürfte jedoch eine Zugriffsbegrenzung auf einen Straftatenkatalog besonders schwerwiegender Taten erforderlich sein.[10] Diesen Voraussetzungen wird § 100g Abs. 2 Satz 2 StPO ohne weiteres gerecht.

4. Reichweite

Die rechtspolitische Diskussion verengt sich oftmals auf die Speicherung von IP-Adressen. In technischer Hinsicht setzen die Telekommunikationsanbieter unterschiedliche Verfahren ein, um eine IP(v4)-Adresse unterschiedlichen Nutzern zuzuweisen (etwa NAT („network address translation") oder insbesondere im Mobilfunk CGN („carrier grade NAT")). Daher erweist sich die bloße Speicherung der IP-Adresse als unzureichend. Vielmehr sind auch diejenigen technischen Begleitdaten – wie etwa Portnummern – zu speichern, die die Zuordnung einer nach außen durch mehrere Personen genutzten IP-Adresse nach innen zu einem konkreten Anschluss oder Gerät ermöglichen.

IV. Zusammenfassung

Bei näherer Betrachtung des geltenden Rechts der Verkehrsdatenspeicherung für Zwecke der Strafrechtspflege ist eine begrenzte IP-Zuordnung mit dem Recht der Europäischen Union vereinbar. Ihre wesentlichen Bezugspunkte sind bereits jetzt in § 113b Abs. 3 TKG angelegt. Die Norm bedarf lediglich geringfügiger Erweiterung hinsichtlich ihrer Erfassungsreichweite.

7 Zu vgl. Beschluss des Ersten Senats vom 27.05.2020 – 1 BvR 1873/13, Rn. 166 ff.

8 Zu vgl. 1 BvR 1873/13, Rn. 169.

9 Zu vgl. 1 BvR 1873/13, Rn. 175.

10 Geringere Voraussetzungen wohl nach BVerfG 1 BvR 1873/13, Rn. 176 f.

Digitalisierung, Berufsrecht und datenschutzrechtliche Verantwortlichkeit

Viktoria Blumenthal/Sven Braun*

Steuerberater und Wirtschaftsprüfer verarbeiten regelmäßig personenbezogene Daten bei der Erbringung ihrer Leistungen. Beide Berufsgruppen nehmen wegen ihrer berufsrechtlichen Pflichten sowie der damit einhergehenden Eigenverantwortlichkeit und Unabhängigkeit ihrer Tätigkeit die datenschutzrechtliche Rolle eines Verantwortlichen ein. Mit zunehmender Digitalisierung verschwimmt jedoch die Grenze zwischen Kernleistung und weiteren Beratungsleistungen. Die Bandbreite reicht dabei von ausschließlich durch Steuerberater und Wirtschaftsprüfer genutzter Software hin zur Gestaltung von digitalen Angeboten, die eigenständig von Mandanten verwendet werden. Daneben bieten insbesondere Wirtschaftsprüfungsgesellschaften weitere digitale Beratungsleistungen an, die über die Kernleistung der betriebswirtschaftlichen Prüfung hinausgehen. Dieser Beitrag untersucht die Auswirkungen der Digitalisierung beider Berufsgruppen sowie der weiteren Angehörigen einer Wirtschaftsprüfungsgesellschaft und kommt zu dem Ergebnis, dass diese dabei weiterhin als Verantwortliche und nicht als Auftragsverarbeiter agieren.

I. Einleitung

Im Zuge der zunehmenden Digitalisierung von Unternehmen verarbeiten auch Steuerberater und Wirtschaftsprüfer vermehrt personenbezogene Daten ihrer Mandanten in einer Weise, die den Anwendungsbereich des Datenschutzrechts eröffnet. Bei den klassischen Kernleistungen wie der Beratung bei der Erstellung und Abgabe von Steuererklärungen oder der Durchführung von Jahresabschlussprüfungen kommen digitale Werkzeuge zum Einsatz, um Routineaufgaben zu automatisieren und Kontrollen schwerpunktmäßig bei Ausnahmen, Regelverstößen und Stichprobenprüfungen durchzuführen.[1] Hier nehmen Steuerberater und Wirtschaftsprüfer Aufgaben wahr, die sie wegen ihrer berufsrechtlichen Pflichten unabhängig, gewissenhaft, verschwiegen und eigenverantwortlich ausführen.[2] Aufgrund ihrer Eigenverantwortlichkeit agieren Steuerberater und Wirtschaftsprüfer datenschutzrechtlich in der Regel nicht als Auftragsverarbeiter,[3] sondern als Verantwortliche im Sinne der Datenschutzgrundverordnung (DS-GVO)[4] – mit allen damit verbundenen Rechten, aber auch Pflichten. Anders als Wirtschaftsprüfer genießen Steuerberater diesbezüglich mit § 11 Abs. 2 S. 1 und 2 Steuerberatungsgesetz (StBerG) eine ausdrückliche gesetzliche Klarstellung, nach der sie bei der Verarbeitung sämtlicher personenbezogener Daten ihrer Mandanten ihre Aufgabenerfüllung als Verantwortliche wahrnehmen.[5]

Zu den Kernleistungen beider Berufsgruppen kommen im Zuge der Digitalisierung vermehrt weitere Beratungsleistungen hinzu, bei denen ebenfalls personenbezogene Daten verarbeitet werden. Hierzu zählt unter anderem die IT- und Prozessberatung, die digitale Forensik bei der Bekämpfung von Wirtschaftskriminalität oder die Beratung zur Absicherung von informationstechnischen Systemen.[6] Infolgedessen verschwimmt die Grenze zwischen der Kernleistung der Steuerberatung und Wirtschaftsprüfung sowie weiteren Beratungsleistungen zunehmend. Dabei wird auch die datenschutzrechtliche Rolle von Steuerberatern und Wirtschaftsprüfern hinterfragt, wobei in der Praxis bei zunehmender Entfernung von der jeweiligen Kernleistung Mandanten vermehrt eine Auftragsverarbeitung annehmen, um einerseits die Kontrolle über personenbezogene Daten zu behalten und andererseits – so die irrtümliche Annahme – die Übermittlung rechtfertigen zu können.[7] Eine Übermittlung bedarf jedoch einer Rechtfertigungsgrundlage aus Art. 6 DS-GVO, welche gerade nicht durch eine Auftragsverarbeitungsvereinbarung ersetzt werden kann. Der Abschluss einer Auftragsverarbeitungsvereinbarung vermittelt dabei, fälschlicherweise, das Gefühl erhöhter Sicherheit, ohne zu berücksichtigen, dass eine Auftragsverarbeitung – schon unabhängig vom Berufsrecht – eher die Ausnahme als die Regel darstellt; denn allein die faktische Lage und nicht das Vorliegen einer Auftragsverarbeitungsvereinbarung ist hierfür entscheidend. Hinzu kommt die Annahme, dass, wer zweckgebunden agiere, stets Auftragsverarbeiter sei, obwohl selbstverständlich auch ein Verantwortlicher jederzeit das Prinzip der Zweckbindung zu berücksichtigen hat.[8] Dieser Beitrag zeigt, dass die datenschutzrechtliche Rolle von Steuerberatern und Wirtschaftsprüfern entgegen dieser Ansicht auch bei einer Erweiterung des Beratungsangebots im Zuge der Digitalisierung weiterhin grundsätzlich die des Verantwortlichen bleibt.

II. Datenschutzrechtliche Stellung bei der Erbringung von Kernleistungen

Kernaufgabe der Steuerberater ist „im Rahmen ihres Auftrags ihre Auftraggeber in Steuersachen zu beraten, sie zu vertreten und ihnen bei der Bearbeitung ihrer Steuerangelegenheiten und bei der Erfüllung ihrer steuerlichen Pflichten Hilfe zu leisten. Dazu gehören auch die Hilfeleistung in Steuerstrafsachen und in Bußgeldsachen wegen einer Steuerordnungswidrigkeit sowie die Hilfeleistung bei der Erfüllung von

* Viktoria Blumenthal ist Syndikusrechtsanwältin im Bereich Datenschutz und Compliance bei der Deloitte GmbH Wirtschaftsprüfungsgesellschaft in Düsseldorf und berät dort vorwiegend im Bereich des Datenschutzes. Sven Braun arbeitet im Bereich Datenschutz und Compliance bei der Deloitte GmbH Wirtschaftsprüfungsgesellschaft in Düsseldorf.

1 Bspw. Coenen, Rethinking Tax 6.2020, 36.

2 § 57 Abs. 1 StBerG, § 43 Abs. 1 WPO.

3 Wirtschaftsprüferkammer, Leitfaden der WPK zur DS-GVO 2018, Kap. C. 1.

4 Art. 4 Nr. 7 DS-GVO.

5 Siehe auch Kuhls, Kommentar zum Steuerberatungsgesetz, 4. Aufl. 2020, § 11 Rn. 6.

6 Elster, in: Bär/Fischer/Gulden, Informationstechnologien als Wegbereiter für den steuerberatenden Berufsstand, 2016, Kap. 28.

7 Seiter, DuD 2019, 127 (128f.).

8 Art. 5 Abs. 1 lit. b DS-GVO.

Buchführungspflichten, die auf Grund von Steuergesetzen bestehen, insbesondere die Aufstellung von Abschlüssen, die für die Besteuerung von Bedeutung sind, und deren steuerrechtliche Beurteilung."[9] Steuerberater sind befugt, darüber hinaus eine wirtschaftsberatende Tätigkeit auszuüben,[10] und verpflichtet, sämtliche ihrer steuer- und wirtschaftsberatenden Leistungen unabhängig, gewissenhaft, verschwiegen und eigenverantwortlich zu erbringen.[11]

Vor der gesetzlichen Klarstellung in § 11 Abs. 2 StBerG wurden bestimmte Leistungen von Steuerberatern, wie etwa die Lohnbuchhaltung von Unternehmen, sogar von den Datenschutzaufsichtsbehörden uneinheitlich eingeordnet. So hat bspw. der LfDI Baden-Württemberg diese Leistungen als Auftragsverarbeitung klassifiziert,[12] wohingegen das BayLDA die Auffassung vertrat, Steuerberater handelten auch bei der Lohnbuchhaltung als Verantwortliche.[13]

Die Klarstellung in der Neufassung des § 11 StBerG, welche am 18.12.2019 in Kraft trat, wurde vom Gesetzgeber ergänzt, um „die notwendige Rechtssicherheit für alle Beteiligten zu schaffen und so die ordnungsgemäße steuerliche Beratung zu gewährleisten".[14] Zudem ist Ziel der Regelung die Sicherstellung der „berufsrechtlichen Pflichten des Steuerberaters als Berufsgeheimnisträger zur unabhängigen, eigenverantwortlichen, gewissenhaften und verschwiegenen Berufsausübung".[15]

Betrachtet man die datenschutzrechtliche Stellung von Wirtschaftsprüfern und Wirtschaftsprüfungsgesellschaften, stellt sich zunächst die Frage, ob diese von der gesetzlichen Klarstellung in § 11 StBerG ebenfalls erfasst werden. Denn § 11 Abs. 2 S. 2 StBerG bestimmt, dass „die Personen und Gesellschaften nach § 3 [...] bei Verarbeitung sämtlicher personenbezogener Daten ihrer Mandanten Verantwortliche" i.S.d. DS-GVO sind. Zu den in § 3 StBerG enumerierten Personen und Gesellschaften gehören gemäß Nr. 1 Var. 5 auch Wirtschaftsprüfer sowie gemäß Nr. 3 Var. 3 Wirtschaftsprüfungsgesellschaften. § 3 StBerG zählt die dort genannten Personen und Gesellschaften als solche auf, die „zur geschäftsmäßigen Hilfeleistung in Steuersachen" befugt sind. Bei genauerer Betrachtung kommt man also unweigerlich zu der sich anschließenden Fragestellung, ob § 11 Abs. 2 StBerG nur auf die in § 3 StBerG aufgelisteten Personen und Gesellschaften oder auch den dortigen Kontext verweist – mithin ähnlich der bekannten juristischen Problematik, ob es sich bei einem Verweis um eine Rechtsgrund- oder Rechtsfolgenverweisung handelt. Würde der Verweis den Kontext erfassen, folgte hieraus, dass Steuerberater, Wirtschaftsprüfer und sonstige Angehörige von Wirtschaftsprüfungsgesellschaften nur dann als datenschutzrechtlich Verantwortliche tätig würden, wenn sie „geschäftsmäßige Hilfeleistung in Steuersachen" leisten. Dem steht jedoch der Wortlaut des § 11 Abs. 2 S. 2 StBerG entgegen, wonach die datenschutzrechtliche Verantwortlichkeit bei „Verarbeitung *sämtlicher* [Herv. durch die Verf.] personenbezogener Daten" besteht. Darüber hinaus liefe eine solche Auslegung dem Zweck der Vorschrift zuwider, denn der Gesetzgeber wollte gerade Rechtssicherheit erreichen und die berufsrechtlichen Pflichten der genannten Personen und Gesellschaften sichern.

Auch wenn man der hier vertretenen Meinung nicht folgt, dass § 11 Abs. 2 StBerG Anwendung auf Wirtschaftsprüfer und Wirtschaftsprüfungsgesellschaften findet, so ergibt sich aus der Anwendbarkeit der berufsrechtlichen Regelungen dennoch, dass nahezu sämtliche Leistungen im Rahmen datenschutzrechtlicher Eigenverantwortlichkeit erbracht werden.

Die Kernaufgabe von Wirtschaftsprüfern besteht in der betriebswirtschaftlichen Prüfung, insbesondere der Jahresabschlussprüfung nach §§ 316 ff. Handelsgesetzbuch (HGB) und des damit verbundenen Bestätigungsvermerks.[16] Darüber hinaus sind Wirtschaftsprüfer auch zur Beratung in steuerlichen und wirtschaftlichen Angelegenheiten befugt.[17] Diese Aufgaben können es erforderlich machen, personenbezogene Daten zu verarbeiten. Gleichzeitig müssen diese Tätigkeiten, da sie dem Berufsrecht unterfallen, unabhängig, gewissenhaft, verschwiegen und eigenverantwortlich wahrgenommen bzw. ausgeübt werden.[18]

Wirtschaftsprüfer haben die Möglichkeit, sich in Wirtschaftsprüfungsgesellschaften zu organisieren, in denen sie sich auch mit anderen Angehörigen des Berufsrechts, wie vereidigten Buchprüfern, Steuerberatern und Rechtsanwälten, zusammenschließen können.[19] Dabei beschäftigten Wirtschaftsprüfungsgesellschaften freilich auch Personen, die selbst keine Berufsträger sind. Die Regelungen über alle Rechte und Pflichten des Berufsrechts finden jedoch auch auf Wirtschaftsprüfungsgesellschaften, und damit auch ihre weiteren Angehörigen, Anwendung;[20] explizit hervorgehoben sei hier die berufsrechtliche Verschwiegenheitspflicht, einschließlich etwaiger strafrechtlicher Konsequenzen.[21] Kommt es bei der Wahrnehmung der genannten Aufgaben zur Verarbeitung personenbezogener Daten, agieren Wirtschaftsprüfer und andere Angehörige von Wirtschaftsprüfungsgesellschaften aufgrund der berufsrechtlich geforderten Eigenverantwortlichkeit folglich datenschutzrechtlich als eigene Verantwortliche.

III. Digitalisierung und datenschutzrechtliche Verantwortlichkeit

Im Rahmen ihrer Aufgabenerfüllung greifen Steuerberater, Wirtschaftsprüfer und andere Angehörige von Wirtschaftsprüfungsgesellschaften[22] vermehrt auf softwarebasierte Lösungen zurück, die zum Teil auch in einer Cloud betrieben

9 § 33 StBerG.

10 § 57 Abs. 3 Nr. 3 Var. 1 StBerG.

11 § 57 Abs. 1 StBerG.

12 LfDI Baden-Württemberg, 34. Tätigkeitsbericht, Kap. 1.10.

13 BayLDA, FAQ zur DS-GVO zur Auftragsverarbeitung bei Steuerberatern, 20.07.2018. Für eine Übersicht der verschiedenen Positionen siehe Kramer/Schmidt, ZD 2020, 194 ff.

14 BT-Drucksache 19/14909 v. 07.11.2019 S. 59.

15 BT-Drucksache 19/14909 v. 07.11.2019 S. 59.

16 Wirtschaftsprüferkammer, Leitfaden der WPK zur DS-GVO 2018, Kap. C. 1.

17 § 2 Abs. 2, 3 WPO.

18 § 43 Abs. 1 WPO.

19 §§ 28 Abs. 1, 44b WPO.

20 § 56 Abs. 1 WPO.

21 § 50 WPO i.V.m. §§ 203 Abs. 1 Nr. 3, Abs. 4 S. 1, 204, 201 StGB.

22 Im Folgenden werden aus sprachlichen Gründen zum Teil nicht alle drei Gruppen genannt, wobei jedoch stets alle Angehörige einer Wirtschaftsprüfungsgesellschaft gemeint sind, da sie ebenfalls – wie bereits aufgezeigt – den berufsrechtlichen Pflichten unterliegen.

werden. Dies ist einerseits der stetigen Weiterentwicklung von Beratungs- und Prüfwerkzeugen geschuldet, andererseits eine Reaktion auf die Digitalisierung in Unternehmen und die entsprechende Begleitung und Beratung durch Steuerberater und Wirtschaftsprüfer.[23] Im Gegensatz zu selbst gehosteten Angeboten (on-premises), wo die datenschutzrechtliche Verantwortlichkeit in der Regel beim Betreiber verortet ist, scheint die Verantwortlichkeit bei cloud-basierten Angeboten gerade im Kontext der berufsrechtlichen Rahmenbedingungen nicht immer auf den ersten Blick klar zu sein.

Bei Cloud-Angeboten kann in der Nutzung im wesentlichen zwischen Angeboten unterschieden werden, die (1.) nur vom Steuerberater oder Wirtschaftsprüfer für die Erfüllung ihrer Kernaufgaben und weiteren Beratungsleistungen eingesetzt werden, wobei Mandanten mit dem digitalen Angebot nicht in Berührung kommen, (2.) im Rahmen der Aufgabenerfüllung von Mandanten und Steuerberatern und Wirtschaftsprüfern gemeinsam genutzt werden, oder (3.) zwar vom Steuerberater oder Wirtschaftsprüfer gestaltet, betreut und bereitgestellt werden, die Nutzung jedoch voll durch Mandanten erfolgt. Im Folgenden werden die unterschiedlichen Szenarien aus Sicht einer Wirtschaftsprüfungsgesellschaft untersucht.

1. Ausschließliche Nutzung durch Steuerberater und Wirtschaftsprüfer

Steuerberater und Wirtschaftsprüfer entwickeln und nutzen Software, um ihre Beratungs- und Prüfungsleistung zu erbringen. Software unterstützt dabei bei der Erhebung von für den Auftrag erforderlichen Daten, kategorisiert Dokumente und weist ggf. sogar auf Risiken oder fehlende Informationen hin. Mandanten haben unter Umständen keine genaue Kenntnis von der eingesetzten Software und eingesetzten Cloud-Dienstleistern.[24]

Bei der Erfüllung ihrer Aufgaben unterliegen Steuerberater und Wirtschaftsprüfer dem Berufsrecht und treten gegenüber ihren Mandanten folglich datenschutzrechtlich als eigene Verantwortliche auf. Sie verarbeiten personenbezogene Daten, um gesetzlichen Verpflichtungen von Mandanten wie der Durchführung einer Jahresabschlussprüfung oder der Erstellung und Abgabe von Steuererklärungen nachzukommen, oder berechtigte Interessen von Mandanten wie der Rechenschaftslegung der Geschäftsführung von Mandanten gegenüber Gesellschaftern zu erfüllen.[25] Dies gilt auch dann, wenn die Leistungen mittels Cloud-Lösungen erbracht werden, wobei Steuerberater und Wirtschaftsprüfer, wenn sie bei der Verarbeitung personenbezogener Daten ihrer Mandanten Dritte einsetzen, dafür Sorge zu tragen haben, dass diese die Verpflichtungen aus Art. 28 DS-GVO erfüllen.[26]

Es schließt sich die Frage an, ob Berufsgeheimnisträger bei der Wahrnehmung allein oder gemeinsam verantwortlich sind. Eine gemeinsame Verantwortlichkeit nach Art. 26 Abs. 1 DS-GVO ist jedoch alleine schon deshalb nicht anzunehmen, weil das Berufsrecht eine eigene Verantwortlichkeit vorsieht. Eine gemeinsame Festlegung der Zwecke und Mittel einer Verarbeitung ist somit ausgeschlossen, weil diese die berufsrechtliche Regelung unterlaufen würde.[27]

In dieser Konstellation scheidet eine Auftragsverarbeitung schon alleine aufgrund der Weisungsbefugnis des Verantwortlichen gegenüber dem Auftragsverarbeiter aus Art. 28 Abs. 3 S. 2 lit. a DS-GVO aus, die mit der Eigenverantwortlichkeit kollidiert.[28]

2. Gemeinsame Nutzung mit Mandanten

Bei der gemeinsamen Nutzung digitaler Angebote mit Mandanten verändert sich die datenschutzrechtliche Verantwortlichkeit von Wirtschaftsprüfungsgesellschaften nicht. Vielmehr ist anzunehmen, dass beide Parteien als eigenständige Verantwortliche auftreten, wie das folgende Beispiel aus der IT-Beratung zeigt.

Bei der Auswahl, Planung, Anpassung und Implementierung von softwarebasierten Lösungen geht es oftmals um die Ablösung oder Ergänzung bestehender IT-Systeme. Häufig ist in diesem Zuge eine Übertragung von personenbezogenen Daten aus alten in neue Systeme gewünscht. Hierfür ist für die Auswahl und Anpassung des neuen Systems sowie die Übertragung selbst eine genaue Kenntnis der bestehenden Daten erforderlich. Diese Kenntnis wird in der Regel durch eine eigene Analyse der Daten erlangt. In diesem Fall nutzen Mandant und Wirtschaftsprüfungsgesellschaft im Rahmen des Beratungsauftrags gemeinsam dieselben bestehenden Systeme und verarbeiten dieselben personenbezogenen Daten; mitunter sogar für denselben Zweck der Ablösung oder Ergänzung bestehender Software.

Bei einer solchen umfassenden Beratung, die technische wie wirtschaftliche Interessen von Mandanten wahrt, ist davon auszugehen, dass es sich um eine wirtschaftliche Beratung i.S.v. § 2 Abs. 3 Nr. 2 Wirtschaftsprüferordnung (WPO) handelt. Damit ist die Leistung vor dem Hintergrund berufsrechtlicher Regelungen zu erbringen, was auch für die damit einhergehende Verarbeitung personenbezogener Daten gilt. Jedoch wird in der Praxis vermehrt schon allein wegen des für die Beratung nötigen Zugriffs auf personenbezogene Daten reflexartig eine Auftragsverarbeitung angenommen.

Aus rein dogmatischer Sicht kann hier argumentiert werden, dass eine Auftragsverarbeitung erst dann unzulässig wäre, wenn über die Verarbeitung personenbezogener Daten hinaus auch die berufsrechtliche Entscheidungsfreiheit beschränkt würde, was zu einem Konflikt mit der berufsrechtlichen Eigenverantwortlichkeit führen würde.[29] Allerdings kann in der Praxis bereits eine einzelne datenschutzrechtliche Weisung im Rahmen des Auftrags erheblich in die jenseits des Datenschutzrechts bestehende Entscheidungsfreiheit eingreifen. Beispielsweise kann die datenschutzrechtliche Weisung zur Pseudonymisierung dazu führen, dass als Folge keine hinreichend genauen Entscheidungen mehr getroffen werden können.

23 Elster, in: Bär/Fischer/Gulden, Informationstechnologien als Wegbereiter für den steuerberatenden Berufsstand, 2016, Kap. 28.

24 Eine Ausnahme besteht, wenn Cloud-Dienstleistungen eines Dritten exklusiv für ein einziges Mandat genutzt werden, denn dann müssen Mandanten der Nutzung des Dienstleisters zustimmen (§ 50a Abs. 5 WPO).

25 Wirtschaftsprüferkammer, Leitfaden der WPK zur DS-GVO 2018, Kap. C. 1.

26 Bspw. Löschhorn, Rethinking Tax 6.2020, 41 (42f.).

27 Kramer/Schmidt, ZD 2020, 194 (196).

28 Kramer/Schmidt, ZD 2020, 194 (198); Wirtschaftsprüferkammer, Leitfaden der WPK zur DS-GVO 2018, Kap. C. 1.

29 Wirtschaftsprüferkammer, WP/vBP und Auftragsverarbeitung (Art. 4 Nr. 8, 28 DS-GVO), Nachricht vom 13.06.2019.

Um dem zuvorzukommen, wäre im Einzelfall eine praktisch nahezu nicht umsetzbare, präzise Abgrenzung der Auftragsverarbeitung und eigenverantwortlicher Verarbeitung durch die Wirtschaftsprüfungsgesellschaft erforderlich. Vor diesem Hintergrund und angesichts der Tatsache, dass die Verarbeitung der personenbezogenen Daten im Rahmen der wirtschaftlichen Beratung erfolgt, ist typischerweise nicht von einer Auftragsverarbeitung auszugehen. Damit stehen Mandant und Wirtschaftsprüfungsgesellschaft nebeneinander als Verantwortliche. Das Ziel des größtmöglichen Schutzes der personenbezogenen Daten wird auch bei der eigenverantwortlichen Verarbeitung durch Wirtschaftsprüfungsgesellschaften vollumfänglich erreicht, da sie die Pflichten des Verantwortlichen (u.a. Art. 24 DS-GVO) ebenfalls umzusetzen haben. Der Schutz kann aufgrund der Pflicht zur berufsrechtlichen Verschwiegenheit, deren Verletzung gemäß § 203 StGB mit Strafe bedroht ist, sogar als höher eingeschätzt werden.

3. Nutzung ausschließlich durch Mandanten

Die zwei zuvor genannten Szenarien decken die typischen Fälle der Steuerberatung, Wirtschaftsprüfung und sonstige Beratung in wirtschaftlichen Fragen auch im Kontext der Digitalisierung weitestgehend ab. Es kann jedoch auch zu Konstellationen kommen, in denen Wirtschaftsprüfungsgesellschaften im Nachgang ihrer Beratungstätigkeit weiterhin als IT-Dienstleister agieren – bspw. bei der Bereitstellung von Cloud-Anwendungen. Es bleibt offen, ob eine solche IT-Dienstleistung gänzlich ohne begleitende Beratung überhaupt von einer Wirtschaftsprüfungsgesellschaft angeboten werden kann, oder ob es sich nicht vielmehr um eine gewerbliche Leistung handelt.[30]

Daher ist fraglich, ob der Anwendungsbereich der berufsrechtlich geregelten Tätigkeit der Wirtschaftsprüfung, Steuerberatung oder sonstigen wirtschaftlichen Beratung für die Verarbeitung von personenbezogenen Daten eröffnet ist oder ob zumindest im Hinblick auf die Verarbeitung personenbezogener Daten keine eigenverantwortliche Tätigkeit ausgeübt wird.

Eine solche Konstellation könnte bei der Gestaltung einer Cloud-Anwendung, die Mandanten eigenständig nutzen, auftreten. Wird im Rahmen eines wirtschaftlichen Beratungsauftrags, wie im obigen Beispiel, initial eine von einer Wirtschaftsprüfungsgesellschaft entwickelte Cloud-Software bei und mit Mandanten eingeführt, liegt zunächst eine, auch datenschutzrechtlich, eigenverantwortliche Tätigkeit vor. Wenn nun ein Mandant nach Abschluss der initialen Beratung die Cloud-Software weiter nutzt und personenbezogene Daten verarbeitet, ohne weitere Beratungsleistungen von Wirtschaftsprüfungsgesellschaften in Anspruch zu nehmen, für die die Verarbeitung personenbezogener Daten erforderlich ist, kann für diese Phase der Verarbeitung eine Auftragsverarbeitung durch die Wirtschaftsprüfungsgesellschaft in Betracht gezogen werden.

Doch selbst in Ausnahmefällen wie diesen unterliegt eine Wirtschaftsprüfungsgesellschaft ihren berufsrechtlichen Verpflichtungen, sodass stets ein Spannungsverhältnis zwischen Berufs- und Datenschutzrecht bestehen bleibt. Eine mögliche Lösung ist, die IT-Dienstleistung nicht über eine Wirtschaftsprüfungsgesellschaft anzubieten. Ist dies keine Option, sind, um hier vertraglich die berufsrechtlichen Regelungen weitestgehend adäquat abzubilden, vor dem Hintergrund der Auftragsverarbeitung bei der Ausgestaltung der Auftragsverarbeitungsvereinbarung nach Art. 28 Abs. 3 DS-GVO einige Punkte zu beachten.

Zunächst ist zu empfehlen, im Hinblick auf die Verpflichtung zur Vertraulichkeit nach Art. 28 Abs. 3 S. 2 lit. b DS-GVO vertraglich darauf hinzuweisen, dass die bei einer Wirtschaftsprüfungsgesellschaft tätigen Personen mit der berufsrechtlichen Verschwiegenheitspflicht aus §§ 43 Abs. 1, 50 WPO bereits im Sinne der zweiten Alternative „einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen".

Daneben soll der Auftragsverarbeiter nach Art. 28 Abs. 3 S. 2 lit. g DS-GVO die personenbezogenen Daten nach Beendigung des Auftrags entweder löschen oder zurückgeben, sofern keine weitere gesetzliche Aufbewahrungspflicht besteht. Dabei sind Berufsträger nach § 51b Abs. 1 WPO zur Führung von Handakten verpflichtet, in der sie ihre Tätigkeit dokumentieren, wobei eine Aufbewahrungspflicht von bis zu zehn Jahren bestehen kann. Eine Handakte ist grundsätzlich bei der Ausübung einer eigenverantwortlichen Tätigkeit zu führen, die in diesem Szenario gerade nicht unterstellt wird. Hier manifestiert sich das Spannungsfeld von Auftragsverarbeitung und berufsrechtlichen Pflichten besonders klar. Zwar finden verarbeitete personenbezogene Daten nicht zwangsläufig ihren Weg in eine Handakte, sie können jedoch bspw. Teil von internen Arbeitspapieren werden.[31] Auch dieser Fall sollte daher in einer Auftragsverarbeitungsvereinbarung Berücksichtigung finden.

Schließlich ist auf die Einschränkung des Inspektionsrechts nach Art. 28 Abs. 3 S. 2 lit. h DS-GVO hinzuweisen. Das Inspektionsrecht von Aufsichtsbehörden ist gemäß Art. 90 DS-GVO i.V.m. § 29 Abs. 3 Bundesdatenschutzgesetz (BDSG) dann eingeschränkt, wenn die Offenlegung der Information zu einem Verstoß gegen die gesetzlichen Verschwiegenheitspflichten führen würde. Wenn jedoch schon das Recht der Aufsichtsbehörden aufgrund der berufsrechtlichen Verschwiegenheit eingeschränkt ist, muss dies erst recht auch für das Inspektionsrecht des Verantwortlichen gegenüber dem Auftragsverarbeiter gelten (argumentum a fortiori). Das Inspektionsrecht ist daher vertraglich einzuschränken, wenn die Inspektion zu einem Verstoß gegen die Verschwiegenheitspflicht führen könnte. Dies dürfte insbesondere dann der Fall sein, wenn im Rahmen der Kontrolle einer Verarbeitungstätigkeit Informationen über andere Mandanten sichtbar würden – schon die Existenz des Mandatsverhältnisses unterliegt der berufsrechtlichen Verschwiegenheit. So können Vor-Ort-Kontrollen in der Praxis nur in einem sehr eingeschränkten Rahmen ermöglicht werden. Um dennoch eine wirksame Kontrolle im Interesse von Mandanten zu ermöglichen, können sich beide Parteien auf die Vorlage geeigneter Nachweise wie bspw. Zertifizierungen zur Informationssicherheit[32] oder, falls diese nicht in ausreichendem Maße vorliegen sollten, auf eine Kontrolle

30 Siehe zu diesem Thema Aicher/Riedel, IDWlife 07/2020, 600 ff.

31 § 51b Abs. 4 WPO.

32 Gabel/Lutz, in: Taeger/Gabel, DS-GVO BDSG, 3. Aufl. 2019, Art. 28 Rn. 57.

ggf. durch einen gemeinsam gewählten Prüfer, der ebenfalls dem Berufsrecht unterliegt und kein Wettbewerber des Auftragsverarbeiters ist, einigen.

IV. Fazit

Mit zunehmender Digitalisierung verschwimmt die Grenze zwischen klassischer Steuerberatung, Wirtschaftsprüfung und darüber hinausgehende IT-Beratung. In diesem Zuge wird auch die datenschutzrechtliche Rolle von Wirtschaftsprüfungsgesellschaften regelmäßig hinterfragt. Zusammenfassend lässt sich sagen, dass sämtliche Angehörige einer Wirtschaftsprüfungsgesellschaft – unabhängig davon, ob sie selber Berufsträger sind oder nicht – nur in äußerst seltenen Fällen als Auftragsverarbeiter agieren.[33] Zwar ist durchaus nachvollziehbar, dass Mandanten ihre Daten durch den Abschluss einer Auftragsverarbeitungsvereinbarung in größerer Sicherheit wiegen. Jedoch wird hierbei die Ausstrahlung der berufsrechtlichen Pflichten auch auf die Verarbeitung personenbezogener Daten ausgeblendet. Häufig wird übersehen, dass mit der berufsrechtlichen Unabhängigkeit und Eigenverantwortlichkeit und der damit einhergehenden datenschutzrechtlichen Verantwortlichkeit nicht nur gewisse Rechte und Freiheiten, sondern vor allem auch Pflichten einhergehen – personenbezogene Daten dem Grunde nach also keinesfalls unsicherer sind, nur weil die Pflichten in diesem Fall statt in einer Auftragsverarbeitungsvereinbarung in der DS-GVO und dem Berufsrecht normiert sind.

Die Trennung von Berufsrecht und Datenschutzrecht ist rein dogmatisch zwar durchaus überzeugend, mit der Praxis jedoch nicht vereinbar. Eine datenschutzrechtliche Weisung hat nahezu immer auch einen Einfluss auf die Erbringung der „inhaltlichen" Leistung. Aus diesem Grund wäre eine gesetzliche Klarstellung nach dem Vorbild des § 11 Abs. 2 StBerG auch für Wirtschaftsprüfer begrüßenswert. Eine solche Klarstellung würde die Abschlüsse nicht erforderlicher Auftragsverarbeitungsvereinbarungen minimieren, die aus fachlicher Unkenntnis oder einem Missverständnis hinsichtlich der Rechtfertigung von Datenübermittlungen resultieren. Da aus diesen Gründen der Abschluss einer Auftragsverarbeitungsvereinbarung mitunter zur Bedingung für eine Auftragsvergabe gemacht wird, mögen derzeit zudem auf Auftragnehmerseite teilweise wirtschaftliche Überlegungen den reinen berufs- und datenschutzrechtlichen Argumenten in der Praxis vorgezogen werden. Dies könnte durch eine Klarstellung ebenfalls vermieden werden. Wie schon bei Steuerberatern würde „Rechtssicherheit für alle Beteiligten" geschaffen sowie die „berufsrechtlichen Pflichten [...] zur unabhängigen, eigenverantwortlichen, gewissenhaften und verschwiegenen Berufsausübung" gesichert.[34]

33 Siehe oben III. 3.

34 BT-Drucksache 19/14909 v. 07.11.2019 S. 59.

Erlauben die beschränkten Bußgeldrahmen in den § § 51 Abs. 5 KDG, 45 Abs. 5 DSG-EKD die wirksame, verhältnismäßige und abschreckende Sanktion von Kleinstunternehmen und kleinen Unternehmen?

Matthias Vöcking*

Die Europäische Datenschutzgrundverordnung (DS-GVO) sieht bei Verstößen nach Art. 83 Absätze 4, 5 und 6 DS-GVO sehr hohe Bußgelder vor. Erlauben die abgesenkten Bußgeldrahmen in den § § 51 Abs. 5 KDG, 45 Abs. 5 DSG-EKD die wirksame, abschreckende und verhältnismäßige Sanktion von Kleinstunternehmen und kleinen Unternehmen?

I. Einleitung

Die Europäische Datenschutzgrundverordnung (DS-GVO)[1] sieht zum Schutz natürlicher Personen bei der widerrechtlichen Verarbeitung personenbezogener Daten erhebliche Bußgelder vor.

Bei formellen Verstößen[2] sind Bußgelder bis zu 10.000.000,00 Euro möglich. Liegt der weltweite Vorjahresumsatz des verantwortlichen oder auftragsverarbeitenden Unternehmens bei über 500 Millionen Euro, können bis zu zwei Prozent des weltweiten Vorjahresumsatzes festgesetzt werden.

Noch härter ist die Sanktion materieller Verstöße.[3] Die Bußgeldobergrenzen sind verdoppelt.

* Assessor Matthias Vöcking unterstützt als freier Mitarbeiter die Rechtsanwaltskanzlei Warther | Rechtsanwälte in Greven. Daneben entwickelt er Programme zur Stärkung ökonomischer, sozialer und ökologischer Nachhaltigkeit.

1 Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27.04.2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung) ABl. L 119, 04.05.2016, ber. ABL. L 127, 23.05.2018.

2 Art. 83 Abs. 4 DS-GVO.

3 Art. 83 Abs. 5 und 6 DS-GVO.

In jedem Einzelfall stellen die Aufsichtsbehörden sicher, dass die verhängte Geldbuße wirksam, verhältnismäßig und abschreckend ist.[4]

Die kirchlichen Datenschutzbestimmungen begrenzen die Bußgeldhöhe auf 500.000,00 Euro.[5] Erlaubt das geringere mögliche Bußgeld eine wirksame, verhältnismäßige und abschreckende Sanktionierung von Kleinstunternehmen und kleinen Unternehmen?

Im nächsten Abschnitt grenzt der Beitrag Kleinstunternehmen und kleine Unternehmen von mittelgroßen Unternehmen und großen Unternehmen ab. Welche Bedeutung haben Kleinstunternehmen und kleine Unternehmen?

Abschnitt III stellt das Konzept der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder zur Bußgeldzumessung in Verfahren gegen Unternehmen vor. Welche Entscheidungen lassen sich für die kirchlichen Verfahren übernehmen? Was sollte bei Konzentration auf Kleinstunternehmen und kleine Unternehmen verändert werden?

In Abschnitt IV wird ein kirchliches Verfahren, ausgerichtet auf Kleinstunternehmen und kleine Unternehmen, vorgestellt. Welche Konsequenz hat die Abweichung vom Verfahren der unabhängigen Datenschutzaufsichtsbehörden?

Abschnitt V fasst das Ergebnis zusammen.

II. Die Abgrenzung von Kleinstunternehmen und kleinen Unternehmen von mittelgroßen und großen Unternehmen

Bei der Abgrenzung der Unternehmensgrößen legen die unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder die Vorjahresumsatzhöhe für die Abgrenzung zugrunde.[6]

„Die unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder sind der Auffassung, dass in einem modernen Unternehmenssanktionsrecht mit erheblichen maximalen Bußgeldbeträgen, das sich zugleich an eine Vielfalt unterschiedlich großer Unternehmen richtet, der Umsatz eines Unternehmens eine geeignete, sachgerechte und faire Anknüpfung zur Sicherstellung der Wirksamkeit, Verhältnismäßigkeit und Abschreckung darstellt."[7]

Danach haben Kleinstunternehmen einen Jahresumsatz bis 2 Millionen Euro. Kleine Unternehmen haben einen Umsatz über 2 Millionen Euro bis 10 Millionen Euro. Der Umsatz Mittlerer Unternehmen liegt über 10 Millionen Euro bis 50 Millionen Euro. Große Unternehmen haben einen Umsatz von über 50 Millionen Euro.

Die tatsächliche Bedeutung der Kleinstunternehmen und Kleinen Unternehmen lässt sich aus der Umsatzsteuerstatistik nachvollziehen.[8]

Danach waren 2018 in Deutschland 3.279.136 umsatzsteuerpflichtige Unternehmen. Davon hatten 570 Unternehmen einen Umsatz von mindestens 1 Mrd. Euro. Weitere 708 Unternehmen hatten einen Umsatz von 500 Millionen bis unter 1 Mrd. Euro. Für 1.278 Unternehmen (0,039 %) sind die Zwei- und Vierprozentgrenzen des Umsatzes als mögliches Bußgeld unmittelbar relevant. Einen Umsatz von 250 Millionen Euro bis unter 500 Millionen Euro haben 1.489 Steuerpflichtige. Bei 4.105 Steuerpflichtigen lag der Umsatz zwischen 100 Millionen Euro und unter 250 Millionen Euro. Einen Umsatz von 50 Millionen Euro bis unter 100 Millionen Euro hatten 6.402 Steuerpflichtige. Danach lag die Anzahl der Großunternehmen bei 13.274 und der Anteil bei 0,4 %.

Mittlere Unternehmen waren 2018 in Deutschland 31.644 mit einem Umsatz von 10 Millionen Euro bis unter 25 Millionen Euro sowie 11.603 Unternehmen mit einem Umsatz von 25 Millionen Euro bis unter 50 Millionen Euro. Das sind 43.247 Steuerpflichtige. Der Anteil liegt bei 1,32 %.

Große und mittlere Unternehmen haben einen Anteil von 1,72 % der Umsatzsteuerpflichtigen. Kleine Unternehmen und Kleinstunternehmen machen demnach 98,28 % der Umsatzsteuerpflichtigen aus.

Maßgeblich ist nach Erwägungsgrund 150 der Datenschutzgrundverordnung der funktionale Unternehmensbegriff. Konzernverbundene Unternehmen können auch bei geringerem Einzelumsatz groß oder mittelgroß sein.

Zahlenmäßig dominieren Einzelunternehmen. Im Jahr 2018 erwirtschafteten 2.155.909 umsatzsteuerpflichtige Einzelunternehmen (65,75 % der umsatzsteuerpflichtigen Unternehmen) Lieferungen und Leistungen von 610,757 Mrd. Euro. Durchschnittlich liegt der Umsatz der Einzelunternehmen bei 283.294,42 Euro. Diese Unternehmen kommen für eine Korrektur nach Erwägungsgrund 150 DS-GVO nicht in Betracht.

III. Das Konzept der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder zur Bußgeldzumessung im Verfahren gegen Unternehmen

Die Datenschutzkonferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (DSK) hat ein Bußgeldzumessungskonzept im Verfahren gegen Unternehmen entwickelt.[9] Es kann fortgelten, bis der Europäische Datenschutzausschuss (EDSA) abschließende Leitlinien zur Methodik der Festsetzung von Geldbußen erlassen hat.[10] Das Bußgeldzumessungskonzept bindet Gerichte nicht, betrifft keine Geldbußen gegen Vereine oder natürliche Personen außerhalb ihrer wirtschaftlichen Tätigkeit. Weder für grenzüberschreitende Fälle noch für andere Datenschutzbehörden der EU ist es bindend.

Die Bußgeldzumessung wird in fünf Schritten erreicht. Im ersten Schritt wird das Unternehmen einer Größenklasse zugeordnet. Vorjahresumsatzabhängig sind die Unternehmen

4 Gleichlautend Art. 83 DS-GVO, §§ 51 Abs. 2 KDG, 45 Abs. 2 DSG-EKD.

5 §§ 51 Abs. 5 KDG, 45 Abs. 5 DSG-EKD.

6 DSK Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder „Konzept der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder zur Bußgeldzumessung in Verfahren gegen Unternehmen" vom 14.10.2019 www.datenschutzkonferenz-online.de>20191016_bußgeldkonzept.pdf.

7 Ebenda II. Bußgeldkonzept Abs. 1.

8 Destatis Statistisches Bundesamt, Fachserie 14 Reihe 8.1 Finanzen und Steuern; Umsatzsteuerstatistik (Voranmeldungen) 2018; erschienen am 24.03.2020; Statistisches Bundesamt (Destatis) 2020; 2 Allgemeiner Überblick; 2.2 Steuerpflichtige und deren Lieferungen und Leistungen 2018 nach Wirtschaftsabschnitten, Größenklassen der Lieferungen und Leistungen, Rechtsform und Ländern.

9 S. Fn. 6.

10 Fn. 6 I Einleitung a.E. S. 2.

zunächst den großen (D), mittelgroßen (C), kleinen (B) und Kleinstunternehmen (A) zugeteilt. Die Kleinstunternehmen und kleinen Unternehmen sind jeweils in drei Untergruppen unterteilt (I-III). Für die großen und die mittelgroßen Unternehmen gibt es jeweils sieben Untergruppen (I-VII).

Für die Bußgeldzumessung ist bis zur Untergruppe D VI der jeweilige mittlere Jahresumsatz der Untergruppe maßgeblich.[11] Die Untergruppe der kleinsten Kleinstunternehmen (A.I) betrifft Unternehmen mit einem Vorjahresumsatz bis 700.000,00 Euro.

Untergruppe	Umsatzobergrenze	Jahresumsatz	Tagessatz[14]
A.I	700.000,00 €	350.000,00 €	972,00 €
A.II	1.400.000,00 €	1.050.000,00 €	2.917,00 €
A.III	2.000.000,00 €	1.700.000,00 €	4.722,00 €
B.I	5.000.000,00 €	3.500.000,00 €	9.722.00 €
B.II	7.500.000,00 €	6.250.000,00 €	17.361,00 €
B.III	10.000.000,00 €	8.750.000,00 €	24.306,00 €
C.I	12.500.000,00 €	11.250.000,00 €	31.250,00 €
C.II	15.000.000,00 €	13.750.000,00 €	38.194,00 €
C.III	20.000.000,00 €	17.500.000,00 €	48.611,00 €
C.IV	25.000.000,00 €	22.500.000,00 €	62.500,00 €
C.V	30.000.000,00 €	27.500.000,00 €	76.389,00 €
C.VI	40.000.000,00 €	35.000.000,00 €	97.222,00 €
C.VII	50.000.000,00 €	45.000.000,00 €	125.000,00 €
D.I	75.000.000,00 €	62.500.000,00 €	173.611,00 €
D.II	100.000.000,00 €	87.500.000,00 €	243.056,00 €
D.III	200.000.000,00 €	150.000.000,00 €	416.667.00 €
D.IV	300.000.000,00 €	250.000.000,00 €	694.444,00 €
D.V	400.000.000,00 €	350.000.000,00 €	972.222,00 €
D.VI	500.000.000,00 €	450.000.000,00 €	1.250.000,00 €

Der zumessungsmaßgebliche mittlere Jahresumsatz liegt für die Untergruppe A.I bei 350.000,00 Euro.[12] Der wirtschaftliche Grundwert entspricht einem Tagessatz. Der maßgebliche Umsatz, bis einschließlich D VI pauschaliert, wird durch 360 geteilt. Ein Tagessatz kostet Unternehmen bis 700.000,00 Euro Jahresumsatz 972,00 Euro.[13]

Die Taten werden als leicht, mittelschwer, schwer oder sehr schwer bewertet. Die Bewertung richtet sich nach den konkreten tatbezogenen Umständen des Einzelfalls (vgl. Art. 83 DS-GVO).[15] Den Kriterienkatalog für die Tatschwere gibt Art. 83 Abs. 2 DS-GVO[16] vor. Dieser lässt sich näher systematisieren. Manche Kriterien wie Art-, Schwere und Dauer des Verstoßes oder das Verschulden betreffen den Verstoß selbst.[17] Weitere Kriterien wie getroffene technische und organisatorische Maßnahmen sowie vorherige Vergehen und aufsichtsbehördliche Maßnahmen betreffen das Vortatverhalten.[18] Der Gesichtspunkt Einhaltung genehmigter Verhaltensregeln und Zertifizierungsverfahren nach Art. 83 Abs. 2 Satz 2 DS-GVO hat in den kirchlichen Regelwerken keine Entsprechung.[19]

Auch das Nachtatverhalten hat Bedeutung. Die DS-GVO hebt hervor die Schadensminderung (Art. 83 Abs. 2 Satz 2 Buchstabe c),[20] die Art und Weise der Kenntniserlangung des Verstoßes (Art. 83 Abs. 3 Satz 2 Buchstabe h),[21] sowie den Umfang der Zusammenarbeit mit der Aufsichtsbehörde (Art. 83 Abs. 2 Buchstabe f).[22,23]

Die bußgeldverhängende Aufsichtsbehörde darf mach Art. 83 Abs. 2 Satz 2 Buchstabe k) auch jeglichen anderen erschwerenden oder mildernden Umstand berücksichtigen. Ein solcher Umstand ist etwa der aus dem Verstoß erlangte wirtschaftliche Vorteil.[24]

Das Bußgeldkonzept differenziert zwischen den formellen Verstößen nach Art. 83 Abs. 4 DS-GVO und materiellen Verstößen nach Art. 83 Absätze 5 und 6 DS-GVO.[25] Für leichte formelle Verstöße sieht das Bußgeldkonzept die Verhängung von ein oder zwei Tagessätzen vor. Bei leichten materiellen Verstößen liegt der Bußgeldrahmen zwischen einem und vier Tagessätzen. Ist ein formeller Verstoß mittelschwer, so setzt die bußgeldverhängende Aufsichtsbehörde ein Bußgeld von zwei bis vier Tagessätzen. Betrifft ein mittelschwerer Verstoß materielle Pflichten, so sind vier bis acht Tagessätze für das Bußgeld vorgesehen. Schwere formelle Verstöße ahndet die Bußgeldstelle mit vier bis sechs Tagessätzen, schwere materielle Verstöße mit acht bis zwölf Tagessätzen Bußgeld.

Sehr schwere formelle Verstöße werden mit mehr als sechs Tagessätzen, sehr schwere materielle Verstöße mit mehr als zwölf Tagessätzen Bußgeld geahndet.

In der letzten Stufe werden insbesondere täterbezogene Umstände oder sonstige Umstände wie eine möglicherweise lange Verfahrensdauer oder drohende Zahlungsunfähigkeit des Unternehmens sowie noch nicht im vierten Schritt berücksichtigte Umstände berücksichtigt und der Betrag entsprechend angepasst.

Bei der Wahl des Multiplikatorfaktors für die Tagessatzanzahl ist zu beachten, der einzelfallbezogene Bußgeldrahmen darf nicht überschritten werden.

IV. Ein kirchliches Bußgeldzumessungsverfahren für die Ahndung von Kleinstunternehmen und kleinen Unternehmen

Mit einem Bußgeldrahmen von bis zu 500.000,00 Euro bemühen sich die Kirchen um eine wirksame, verhältnismäßige und abschreckende Ahndung von bußgeldbewehrten Datenschutzrechtsverstößen.

11 Fn. 6 S. 6 II 2.

12 Fn. 6 S. 6 II 2.: 0 Euro + 700.000,00 Euro: 2.

13 Fn. 6 S. 7 II 3.

14 Tabellen 1 – 3 Bußgeldkonzept S. 3-7.

15 Fn. 6 S. 7-8 II 4; vgl. § 51 KDG, 45 DSG-EKD.

16 Vgl. § 51 Abs. 3 Satz 2 KDG, § 45 Abs. 3 Satz 2 DSG EKD.

17 Art. 83 Abs. 2 Satz 2 Buchstaben a) und b) DS-GVO; § 51 Abs. 3 Satz 2 Buchstaben a) und b) KDG, § 45 Abs. 3 Satz 2 Nr. 1 und 2 DSG-EKD. Zu den Kriterien, die den Verstoß betreffen, s. HK DS-GVO/BDSG, Schwartmann/Jaquemain, Art. 83/§ 41 BDSG Rn. 48-53.

18 Art. 83 Abs. 2 Satz 2 Buchstaben d), e) und i) DS-GVO; § 51 Abs. 3 Satz 2 Buchstaben d), e) und i) KDG, § 45 Abs. 3 Satz 2 Nr. 4, 5 und 9 DSG-EKD; ausführlich hierzu dieselben ebenda Rn. 54-60.

19 Denkbar wären staatlich vermittelte Verhaltensregeln und Zertifizierungsverfahren zum vorbeugenden Rechtsschutz, deren Einhaltung ein niedrigeres Bußgeld rechtfertigen könnte. Zur staatlichen Regelung s. HK DS-GVO/BDSG Schwartmann/Jaquemain, Art. 83 Rn. 59.

20 Vgl. § 51 Abs. 3 Satz 2 Buchstabe c) KDG, § 45 Abs. 3 Satz 2 Nr. 3 DSG-EKD.

21 Vgl. § 51 Abs. 3 Satz 2 Buchstabe h) KDG, § 45 Abs. 3 Satz 2 Nr. 8 DSG-EKD.

22 Vgl. § 51 Abs. 3 Satz 2 Buchstabe f) KDG, 45 Abs. 3 Satz 2 Nr. 6 DSG-EKD.

23 HK DS-GVO/BDSG, Schwartmann/Jaquemain, Art. 83 Rn. 61-65.

24 Dieselben ebenda Rn. 66; vgl. § 51 Abs. 3 Satz 2 Buchstabe j) KDG, § 45 Abs. 3 Satz 2 Nr. 10 DSG-EKD.

25 Tabelle 4 zum Bußgeldkonzept, S. 8.

In jedem Einzelfall stellen die Kirchen, wie auch die DS-GVO, sicher, dass das Bußgeld wirksam, verhältnismäßig und abschreckend ist.

Liegt der weltweite Umsatz des unternehmenstragenden Bußgeldschuldners bei über 500 Mio. Euro, so sind bis zu zwei Prozent oder bis zu vier Prozent des weltweiten Vorjahresumsatzes als Bußgeld festsetzbar.[26] Auch in diesen Fällen, wie in jedem Einzelfall, ist das Bußgeld wirksam, verhältnismäßig und abschreckend.

Auf Grundlage deutscher Strafrechtsdogmatik ist ein abstraktes Gewährleisten verhältnismäßiger und abschreckender Sanktion undurchführbar. Alle fünf Strafsenate des Bundesgerichtshofs beschränken Abschreckung als Strafzweck auf den Einzelfall.[27] Die Tatsacheninstanz muss feststellen, dass Straftaten wie die abgeurteilte Straftat oder ähnliche Straftaten gemeinwohlgefährlich zugenommen haben. Abschreckende Sanktion ist danach nur im Ausnahmefall verhältnismäßig. Abschreckung in jedem Einzelfall ist unverhältnismäßig.

Besser als „Abschreckung" lässt sich der Gedanke der Rechtsbewährung vermitteln. Eine Strafzumessungsentscheidung ist rechtsfehlerhaft, wenn sich die verhängte Strafe nach oben oder unten von ihrer Bestimmung löst, gerechter Schuldausgleich zu sein.[28]

Dagegen sensibilisiert die Rechtsprechung bei der Aussetzungsentscheidung, ob sie die Rechtstreue einer über die Besonderheiten des Einzelfalls aufgeklärten Bevölkerung beeinträchtigen und die Strafaussetzung von der Allgemeinheit als ungerechtfertigtes Zurückweichen vor der Kriminalität angesehen werden kann.[29]

Solange eine wirksame und verhältnismäßige Sanktionsentscheidung zur Rechtstreue über die Besonderheiten des Einzelfalls Aufgeklärter beiträgt, muss sie sich nicht auf „Abschreckung" stützen. Tut sie es, schadet die Falschbezeichnung „Abschreckung" statt „Rechtsbewährung" nicht.

Wenigstens wenn der weltweite Umsatz des unternehmenstragenden Bußgeldschuldners bei über 500 Millionen Euro liegt, gewährleistet ein Abschöpfen von bis zu zwei oder vier Prozent des Umsatzes eine wirksame, verhältnismäßige und abschreckende Sanktion.

Hieran kann sich ein wesentlich auf Kleinstunternehmen und kleine Unternehmen konzentriertes kirchliches Bußgeldverfahren orientieren. Es knüpft wie die Bußgeldordnung der unabhängigen Aufsichtsbehörden oder die DS-GVO bei den sehr großen Unternehmen an den Vorjahresumsatz an.

Nach Erwägungsgrund 13 Satz 4 sind Organe und Einrichtungen der Union sowie die Mitgliedstaaten und deren Aufsichtsbehörden dazu angehalten, bei der Anwendung dieser Verordnung die besonderen Bedürfnisse von Kleinstunternehmen sowie von kleinen und mittleren Unternehmen (=KMU) zu berücksichtigen. Die Rücksicht auf besondere Bedürfnisse schließt ein Diskriminierungsverbot bei der Rechtsanwendung ein. Dieses bindet auch den Europäischen Datenschutzausschuss. Ein Bußgeld auf Grundlage von mehr Tagessätzen oder einer ungünstigeren Tagessatzbildung diskriminiert KMU. Es widerspricht Erwägungsgrund 13 Satz 4. Was den größten Großunternehmen recht ist, ist den KMU billig.

Die Bestimmung der Untergruppen und die Veranlagung der Tagessätze auf Grundlage des mittleren Jahresumsatzes der Untergruppe sollte vermieden werden. Laut Umsatzsteuerstatistik 2018 gehört ein Unternehmen mit einem Vorjahresumsatz von 250.000,00 Euro bereits zum Drittel der größten Umsatzsteuerschuldner.[30] Dennoch wird es auf Basis der Untergruppe der kleinsten Kleinstunternehmen mit 140 % seines tatsächlichen Umsatzes veranschlagt.[31] Der Maßstab für die Sanktionierung ist typisiert. Eine Typisierung muss sich realitätsgerecht am typischen Fall orientieren.[32] Eine alle Unternehmen mit einem Vorjahresumsatz bis 700.000,00 Euro auf Grundlage von 350.000,00 Euro typisierende Regelung typisiert nicht realitätsgerecht am typischen Fall. Mehr als zwei Drittel aller Umsatzsteuerpflichtigen setzen weniger als 250.000,00 Euro im Jahr um.

Die Heranziehung von mehr als dem tatsächlichen Vorjahresumsatz für die Beurteilung verschärft eine bereits abschreckende Regelung. Ihre Verhältnismäßigkeit steht in Frage, wenn die mildere Sanktion auf Grundlage des tatsächlichen Vorjahresumsatzes bereits abschreckt. Auch die Rechtstreue mit den Umständen des Falles Vertrauter kann so nicht gefördert werden. Sie leidet.

Bei Unternehmen mit mehr als 500 Mio. Euro Vorjahresumsatz entsprechen die Faktoren 7,2 und 14,4 zugleich den in Art. 83 Abs. 4 und Abs. 5 festgelegten Höchstgrenzen von 2 % und 4 % des Vorjahresumsatzes.[33]

Bei einem Unternehmen mit einem Vorjahresumsatz von 250.000,00 Euro wird bei Festsetzung der Höchstsanktion für schwere Verfehlungen (sechs oder zwölf Tagessätze) bereits ein größerer Teil des tatsächlichen Vorjahresumsatzes abgeschöpft. Die Faktoren liegen bei 8,4 und 16,8.[34] Die Typisierung begründet ein unaufhebbares Spannungsverhältnis von Abschreckung und Verhältnismäßigkeit. Auch die den kleineren 2/3 zugehörenden Unternehmen müssen ohne Diskrimi-

26 Art. 83 Abs. 4-6 DS-GVO.

27 BGH, Beschl. des Ersten Strafsenates v. 07.03.2018 – Az. 1 StR 663/17 7, NStZ-RR 2018, 170; Beschl. des Zweiten Strafsenates v. 10.08.2005 – 2 StR 219/05 5, StraFO, 2005, 515; Beschl. des Dritten Strafsenates v. 23.11.2010 – 3 StR 393/10, NStZ-RR 2013, 102; Beschl. des Vierten Strafsenates vom 08.05.2007 – 4 StR 173/07, NStZ-RR 2007, 702; Beschl. des Fünften Strafsenates v. 11.04.2013 – 5 StR 113/13, NStZ-RR 2013, 240.

28 BGH, Urt. v. 06.07.2017 – 4 StR 415/16, Urteilsrn. 15.

29 BGH, Urt. v. 06.07.2017 – 4 StR 415/16, Urteilsrn. 31.

30 Fn. 8: Von 3.279.136 Steuerpflichtigen entfielen 840.448 (25,63 %) auf einen Umsatz über 17.500,00 Euro bis unter 50.000,00 Euro. Es entfielen 633.316 Steuerpflichtige (19,31 %) auf einen Umsatz über 50.000,00 Euro bis unter 100.000,00 Euro. Auf einen Umsatz von 100.000,00 Euro bis unter 250.000,00 Euro entfielen 731.576 Steuerpflichtige (22,31 %). Mehr als zwei Drittel der Umsatzsteuerpflichtigen (67,25 %) hatten einen Umsatz von unter 250.000,00 Euro.

31 Zumessungsmaßgeblicher mittlerer Jahresumsatz 350.000,00 Euro: tatsächlicher Umsatz 250.000,00 Euro = 140 % des tatsächlichen Umsatzes.

32 BVerfG, Urt. v. 10.04.2018 – 1 BvL 11/14, Juris, Rn. 136; f. Für Bußgeldbemessungen werden insoweit keine milderen Maßstäbe als für die Steuer gelten.

33 HK DS-GVO/BDSG, Schwartmann/Jaquemain, Art. 83 Rn. 97.

34 Nominale Tagessatzzahl X 1,4 aufgrund Heranziehung des Unternehmens mit 140 % seines Vorjahresumsatzes = effektive Tagessatzzahl. Die Sanktionsempfindlichkeit ist Zumessungskriterium, vgl. BGH, Beschl. v. 04.07.2007 – 2 StR 270/07, NStZ-RR 2007, 300.

nierung mit dem Mindestbußgeld für sehr schwere Verstöße sanktioniert werden können.

Bei einem Unternehmen mit einem Vorjahresumsatz von 500.000,00 Euro wird dieser nur zu 70 % angesetzt.[35] Es muss mit der Mindestsanktion für sehr schwere Verstöße geahndet werden können, um die wirksame, verhältnismäßige und abschreckende Sanktionierung in jedem Einzelfall zu gewährleisten. Die Mindestsanktionen liegen bei über sechs oder über zwölf Tagessätze. Auf Grundlage des fiktiven Vorjahresumsatzes müssten die Sanktionen liegen bei über acht oder über 17 Tagessätzen.[36] Das wäre diskriminierend.

Sehr große Unternehmen erfahren eine geringere Abschöpfung von höchstens 2 % oder 4 % des Vorjahresumsatzes. Bei Unternehmen mit einem Vorjahresumsatz von über 500.000,00 Euro bis 700.000,00 Euro sind mehr Tagessätze auf den 350.000,00 Euro Pauschalumsatz nötig, um bei sehr schwerem Verstoß effektiv die Mindestsanktion durchzusetzen.

Auf Basis des tatsächlichen Vorjahresumsatzes sind bis zu 7,2 und 14,4 Tagessätze wirksam, verhältnismäßig und abschreckend. Sie sind bei Berücksichtigung der geringen Höchsttagessatzanzahl einerseits und der möglichen Verwarnung anstelle eines Bußgeldes bei geringfügigen Verstößen auch von Unternehmen[37] andererseits nicht unverhältnismäßig.

Die kirchlichen Bußgeldrahmen von bis zu 500.000,00 Euro lassen eine Sanktionierung von Kleinstunternehmen, kleinen Unternehmen sowie von mittelgroßen Unternehmen mit einem Umsatz bis zu 12.500.000,00 Euro uneingeschränkt zu. 12.500.000,00 Euro Vorjahresumsatz X 0,04 = 500.000,00 €.

Mittelgroße Unternehmen mit einem Vorjahresumsatz von über 12.500.000,00 Euro bis 25.000.000,00 Euro können eingeschränkt sanktioniert werden. Die Sanktion auch schwerer formeller Verstöße und mittelschwerer materieller Verstöße ist möglich. Schwere formelle Verstöße sind mit einem Bußgeld von höchstens sechs Tagessätzen bedroht. Bei mittelschweren materiellen Verstößen drohen bis zu acht Tagessätze Geldbuße. Bis zu zwei Prozent des Vorjahresumsatzes von 25.000.000,00 Euro können mit einem Bußgeld von 500.000,00 Euro abgeschöpft werden. Das entspricht 7,2 Tagessätzen.

Nach dem Bußgeldzumessungskonzept der unabhängigen Aufsichtsbehörden wird ein Unternehmen mit einem Vorjahresumsatz von 25.000.000,00 Euro nur aufgrund des mittleren Jahresumsatzes der Untergruppe veranschlagt. Dieser mittlere Jahresumsatz der Untergruppe C.IV liegt bei 22.500.000,00 Euro. Acht Tagessätze auf Basis des mittleren Jahresumsatzes entsprechen 7,2 Tagessätzen auf Basis des tatsächlichen Umsatzes. Der fiktive Umsatz im Bußgeldzumessungskonzept ist gegenüber dem tatsächlichen Umsatz um 10 % vermindert. Dies wird durch die Abschöpfung des 7,2-fachen Tagessatzes anstelle des achtfachen vom Fiktivumsatz bei der Bußgeldhöhe genau ausgeglichen. Eine wirksame, abschreckende und verhältnismäßige Sanktion auch mittelschwerer materieller Verstöße ist möglich. In beiden Fällen liegt das Bußgeld bei 500.000,00 Euro.

Größere Unternehmen mit über 25.000.000,00 Euro Jahresumsatz sollten aufgrund des öffentlichen Interesses an ihnen (Rechtsbewährung) nach staatlichen Bußgeldregeln sanktioniert werden. Gleiches gilt für mittelgroße Unternehmen mit einem Vorjahresumsatz von über 12.500.000,00 Euro, wenn ihnen ein sehr schwerer Verstoß oder wenigstens ein schwerer materieller Verstoß vorzuwerfen ist.

V. Ergebnis

Auf Basis der von der DS-GVO für Unternehmen mit einem Weltumsatz von über 500 Mio. Euro als wirksam, verhältnismäßig und abschreckend bestimmten Sanktionierung können Kleinstunternehmen, Kleine Unternehmen und mittelgroße Unternehmen mit einem Vorjahresumsatz bis 12.500.000,00 Euro auf Basis der kirchlichen Bußgeldrahmen uneingeschränkt sanktioniert werden.

Mittelgroße Unternehmen mit einem Vorjahresumsatz von über 12.500.000,00 Euro bis 25.000.000,00 Euro können auch noch für schwere formelle Verstöße oder mittelschwere materielle Verstöße wirksam, abschreckend und verhältnismäßig sanktioniert werden.

Nur größere Unternehmen und die mittelgroßen mit einem Vorjahresumsatz von über 12.500.000,00 Euro bei sehr schweren oder wenigstens schweren materiellen Verstößen sollten aufgrund des öffentlichen Interesses an ihnen (Rechtsbewährung) nach staatlichem Recht sanktioniert werden.

Allein aufgrund von Größe scheiden aus dem kirchlichen Bußgeldrahmen 24.877 umsatzsteuerpflichtige Unternehmen aus. Das sind bei 3.279.136 umsatzsteuerpflichtigen Unternehmen 0,76 %. Von 31.677 umsatzsteuerpflichtigen Unternehmen mit einem Vorjahresumsatz von über 10 Millionen Euro bis unter 25 Millionen Euro können Unternehmen bis zu einem Vorjahresumsatz von 12.500.000,00 Euro uneingeschränkt sanktioniert werden. Bei größerem Umsatz bis 25 Millionen Euro ist eine eingeschränkte Sanktionierung möglich und zweckmäßig.

Der Umsatz ist für die größten Unternehmen durch die DS-GVO sowie von den selbständigen Aufsichtsbehörden als taugliche Grundlage bestätigt worden. Dem können sich die kirchlichen Bußgeldzumessungen anschließen.

Allein im Rahmen der pauschalierten Behandlung der Untergruppe der kleinsten Kleinstunternehmen (A.I) wird die Mehrzahl der Umsatzsteuerpflichtigen deutlich zu hoch bewertet. Die Pauschalierung löst sich gerade hier von der realitätsgerechten Orientierung am Regelfall. Dies kann die Rechtstreue mit den Umständen des Einzelfalles Vertrauter beeinträchtigen.

Die Unternehmen sollten jeweils mit ihrem tatsächlichen Umsatz beurteilt werden. Dies vermeidet eine Verschärfung einer bereits abschreckenden Sanktionierung. Es droht die Verwerfung der Regelungen als unverhältnismäßig. Die weitere Verschärfung einer abschreckenden Sanktion kann nicht mehr verhältnismäßig sein. Sie ist nicht erforderlich und unangemessen.

35 Laut Umsatzsteuerstatistik hatten 2018 395.995 Steuerpflichtige einen Umsatz von 250.000 bis 500.000 Euro. Bei insgesamt 3.279.136 Umsatzsteuerpflichtigen liegt der Anteil bei 12,08 %. Von den 273.465 Steuerpflichtigen mit einem Umsatz von 500.000,00 Euro bis unter 1.000.000,00 Euro (8,34 %) werden die Steuerpflichtigen mit einem Umsatz bis 700.000,00 Euro noch stärker entlastet. Die Steuerpflichtigen mit einem Umsatz über 700.000,00 Euro bis unter 1.000.000,00 Euro werden dagegen in der zweiten Untergruppe mit einem pauschalierten Umsatz von 1.050.000,00 Euro überschätzt.

36 Nominale Tagessatzzahl: 0,7 aufgrund Heranziehung des Unternehmens mit 70 % des tatsächlichen Vorjahresumsatzes.

37 Erwägungsgrund 148.

Rechtsprechung

Anforderungen an den Nachweis einer wirksamen Datenschutz-Einwilligung (Ls)

(**Europäischer Gerichtshof**, Urteil vom 11. November 2020 – C-61/19 –)

Art. 2 Buchst. h und Art. 7 Buchst. a der Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr sowie Art. 4 Nr. 11 und Art. 6 Abs. 1 Buchst. a der Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung) sind dahin auszulegen, dass es dem für die Verarbeitung von Daten Verantwortlichen obliegt, nachzuweisen, dass die betroffene Person ihre Einwilligung in die Verarbeitung ihrer personenbezogenen Daten durch aktives Verhalten bekundet hat und dass sie vorher eine Information über alle Umstände im Zusammenhang mit dieser Verarbeitung in verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache erhalten hat, die sie in die Lage versetzt, die Konsequenzen dieser Einwilligung leicht zu ermitteln, so dass gewährleistet ist, dass die Einwilligung in voller Kenntnis der Sachlage erteilt wird. Ein Vertrag über die Erbringung von Telekommunikationsdiensten, der die Klausel enthält, dass die betroffene Person über die Sammlung und die Aufbewahrung einer Kopie ihres Ausweisdokuments mit Identifikationsfunktion informiert worden ist und darin eingewilligt hat, ist nicht als Nachweis dafür geeignet, dass diese Person ihre Einwilligung in die Sammlung und Aufbewahrung dieser Dokumente im Sinne dieser Bestimmungen gültig erteilt hat, wenn

- **das Kästchen, das sich auf diese Klausel bezieht, von dem für die Verarbeitung der Daten Verantwortlichen vor Unterzeichnung dieses Vertrags angekreuzt worden ist oder wenn**
- **die Vertragsbestimmungen dieses Vertrags die betroffene Person über die Möglichkeit, den Vertrag abzuschließen, auch wenn sie sich weigert, in die Verarbeitung ihrer Daten einzuwilligen, irreführen können oder wenn**
- **die freie Entscheidung, sich dieser Sammlung und Aufbewahrung zu widersetzen, von diesem Verantwortlichen ungebührlich beeinträchtigt wird, indem verlangt wird, dass die betroffene Person zur Verweigerung ihrer Einwilligung ein zusätzliches Formular unterzeichnet, in dem diese Weigerung zum Ausdruck kommt.**

Reichweite der Privatsphäre bei Presseberichterstattung über Beerdigung (Ls)

(**Bundesgerichtshof**, Urteil vom 10. November 2020 – VI ZR 62/17 –)

Das durch Art. 2 Abs. 1, Art. 1 Abs. 1 GG, Art. 8 Abs. 1 EMRK gewährleistete Recht auf Achtung der Privatsphäre gesteht jedermann einen autonomen Bereich der eigenen Lebensgestaltung zu, in dem er seine Individualität unter Ausschluss anderer entwickeln und wahrnehmen kann. Dazu gehört auch das Recht, für sich zu sein, sich selbst zu gehören und den Einblick durch andere auszuschließen. Der Schutz der Privatsphäre ist sowohl thematisch als auch räumlich bestimmt. Er umfasst insbesondere Angelegenheiten, die wegen ihres Informationsgehalts typischerweise als „privat" eingestuft werden, etwa weil ihre öffentliche Erörterung oder Zurschaustellung als unschicklich gilt, das Bekanntwerden als peinlich empfunden wird oder nachteilige Reaktionen der Umwelt auslöst. Dazu gehören grundsätzlich auch – regelmäßig in Abhängigkeit von Detailreichtum und Tiefe der Information – Vorfälle aus dem Familienbereich, die Ausgestaltung familiärer Beziehungen wie auch Situationen großer emotionaler Belastung wie bei der Trauer um einen Angehörigen oder eine nahestehende Person, da sie Gefühlsäußerungen, persönliche Regungen und Handlungen auslösen können, die erkennbar nicht für die Augen Dritter bzw. Unbeteiligter bestimmt sind.

Entgeltgleichheitsklage: Vermutung der Benachteiligung wegen des Geschlechts bei Entgeltgleichheitsklage

(**Bundesarbeitsgericht**, Urteil vom 21. Januar 2021 – 8 AZR 488/19 –)

Klagt eine Frau auf gleiches Entgelt für gleiche oder gleichwertige Arbeit, begründet der Umstand, dass ihr Entgelt geringer ist als das vom Arbeitgeber mitgeteilte Vergleichsentgelt (Median-Entgelt) der männlichen Vergleichspersonen, regelmäßig die – vom Arbeitgeber widerlegbare – Vermutung, dass die Benachteiligung beim Entgelt wegen des Geschlechts erfolgt ist.

Sachverhalt:*

Die Klägerin ist bei der Beklagten als Abteilungsleiterin beschäftigt. Sie erhielt im August 2018 von der Beklagten eine Auskunft nach §§ 10 ff. EntgTranspG, aus der ua. das Vergleichsentgelt der bei der Beklagten beschäftigten männlichen Abteilungsleiter hervorgeht. Angegeben wurde dieses entsprechend den Vorgaben von

§ 11 Abs. 3 EntgTranspG als „auf Vollzeitäquivalente hochgerechneter statistischer Median" des durchschnittlichen monatlichen übertariflichen Grundentgelts sowie der übertariflichen Zulage (Median-Entgelte). Das Vergleichsentgelt liegt sowohl beim Grundentgelt als auch bei der Zulage über dem Entgelt der Klägerin. Mit ihrer Klage hat die Klägerin die Beklagte – soweit für das Revisionsverfahren von Interesse – auf Zahlung der Differenz zwischen dem ihr gezahlten Grundentgelt sowie der ihr gezahlten Zulage und der ihr mitgeteilten höheren Median-Entgelte für die Monate August 2018 bis Januar 2019 in Anspruch genommen.

Das Arbeitsgericht hat der Klage stattgegeben. Das Landesarbeitsgericht hat das Urteil des Arbeitsgerichts auf die Berufung der Beklagten abgeändert und die Klage abgewiesen. Es hat angenommen, es lägen schon keine ausreichenden Indizien iSv. § 22 AGG vor, die die Vermutung begründeten, dass die Klägerin die Entgeltbenachteiligung wegen des Geschlechts erfahren habe.

Die Revision der Klägerin hatte vor dem Achten Senat des Bundesarbeitsgerichts Erfolg.

Aus den Gründen:

Mit der vom Landesarbeitsgericht gegebenen Begründung durfte die Klage nicht abgewiesen werden. Aus der von der Beklagten erteilten Auskunft ergibt sich das Vergleichsentgelt der maßgeblichen männlichen Vergleichsperson. Nach den Vorgaben des EntgTranspG liegt in der Angabe des Vergleichsentgelts als Median-Entgelt durch einen Arbeitgeber zugleich die Mitteilung der maßgeblichen Vergleichsperson, weil entweder ein konkreter oder ein hypothetischer Beschäftigter des anderen Geschlechts dieses Entgelt für gleiche bzw. gleichwertige Tätigkeit erhält. Die Klägerin hat gegenüber der ihr von der Beklagten mitgeteilten männlichen Vergleichsperson eine unmittelbare Benachteiligung iSv. § 3 Abs. 2 Satz 1 EntgTranspG erfahren, denn ihr Entgelt war geringer als das der Vergleichsperson gezahlte. Entgegen der Annahme des Landesarbeitsgerichts begründet dieser Umstand zugleich die – von der Beklag-ten widerlegbare – Vermutung, dass die Klägerin die Entgeltbenachteiligung „wegen des Geschlechts" erfahren hat. Aufgrund der bislang vom Landesarbeitsgericht getroffenen Feststellungen konnte der Senat nicht entscheiden, ob die Beklagte, die insoweit die Darlegungs- und Beweislast trifft, diese Vermutung den Vorgaben von § 22 AGG in unionsrechtskonformer Auslegung entsprechend widerlegt hat. Zugleich ist den Parteien Gelegenheit zu weiterem Vorbringen zu geben. Dies führte zur Aufhebung der angefochtenen Entscheidung und zur Zurückverweisung der Sache zur neuen Verhandlung und Entscheidung an das Landesarbeitsgericht.

*(*Auszug der BAG-PM 1/21)*

Zur Verhinderung der Ausübung eines Amts als Personalratsmitglied nach strittiger außerordentlicher Kündigung (Ls)

(**Bundesverwaltungsgericht**, Beschluss vom 4. Februar 2021 – 5 VR 1.20 –)

1. **Ein dem Personalrat angehörender Arbeitnehmer, der nach der außerordentlichen Kündigung seines Arbeitsverhältnisses ein Kündigungsschutzverfahren einleitet, darf in der Ausübung seines Personalratsamtes nicht behindert werden, wenn er glaubhaft machen kann, dass die angegriffene Kündigung offensichtlich unwirksam ist.**

2. **Lässt sich die offensichtliche Unwirksamkeit der außerordentlichen Kündigung nicht feststellen, geht die rechtliche Ungewissheit über den Fortbestand des Arbeitsverhältnisses und der davon abhängenden Mitgliedschaft im Personalrat dergestalt zu Lasten des gekündigten Personalratsmitglieds, dass dieses bis auf Weiteres (nach § 31 Abs. 1 Satz 2 BPersVG) aus rechtlichen Gründen an der Ausübung seines Amtes verhindert ist.**

(Nicht amtliche Leitsätze)

Anspruch der Presse auf Auskunft aus den Akten eines abgeschlossenen Disziplinarverfahrens (Ls)

(**Bundesverwaltungsgericht**, Urteil vom 13. Oktober 2020 – 2 C 41.18 –)

1. **Der Anspruch der Presse auf Auskunft zu einem behördlichen Disziplinarverfahren gegen einen Bundesbeamten findet seine Grundlage im Personalaktenrecht in § 111 Abs. 2 Satz 1 Nr. 2 BBG.**

2. **Das disziplinarrechtliche Verwertungsverbot und das Tilgungsgebot (§ 16 Abs. 1 und 3 BDG) sind als bedeutsame Abwägungsfaktoren auf Seiten des Rechts auf informationelle Selbstbestimmung des betroffenen Beamten in die nach § 111 Abs. 2 Satz 1 Nr. 2 BBG vorzunehmende Interessenabwägung einzustellen.**

3. **Das Merkmal „zwingend erforderlich" des § 111 Abs. 2 Satz 1 Nr. 2 BBG ist im Lichte der Pressefreiheit dahin auszulegen, dass die Auskunftserteilung nicht von einer inhaltlichen Bewertung des Informationsanliegens abhängt. Nicht „zwingend erforderlich" kann eine von der Presse verlangte Information sein, wenn sie aus anderen öffentlich zugänglichen Informationsquellen anderweitig verfügbar ist.**

4. **Die während eines Verwaltungs- oder Klageverfahrens mit dem Ablauf der Tilgungsfrist entstehende Pflicht des Dienstherrn, die Disziplinarakte von Amts wegen zu vernichten, tritt mit seiner Pflicht, die von einem Dritten geltend gemachte Auskunft gegebenenfalls erteilen zu müssen, in Konflikt. Der Ausgleich der kollidierenden Rechtspflichten des Dienstherrn kann nur dadurch hergestellt werden, dass der Disziplinarvorgang bis zur bestands- oder rechtskräftigen Entscheidung über das Auskunftsersuchen in eine gesonderte Aufbewahrung genommen wird.**

Außerordentliche Kündigung wegen unberechtigter Datenlöschung in erheblichem Umfang

(**Landesarbeitsgericht Baden-Württemberg**, Urteil vom 17. September 2020 – 17 Sa 8/20 –)

Löscht ein Arbeitnehmer im Anschluss an ein Personalgespräch, in dem der Arbeitgeber den Wunsch äußerte, sich vom Arbeitnehmer trennen zu wollen, vom Server des Arbeitgebers Daten in erheblichem Umfang (hier: 7,48 GB), nachdem er sich von einer Mitarbeiterin (Einkäuferin) mit den Worten „man sieht sich immer zweimal im Leben" verabschiedet hatte, rechtfertigt dies die außerordentlich fristlose Kündigung des Arbeitsverhältnisse.

Aus den Gründen:

Die Löschung von Daten auf dem Server der Beklagten stellt an sich einen wichtigen Kündigungsgrund dar.

(1) Als wichtiger Grund ist neben der Verletzung vertraglicher Hauptpflichten auch die schuldhafte Verletzung von Nebenpflichten „an sich" geeignet (vgl. BAG 8. Mai 2014 – 2 AZR 249/13 – Rn. 19, AP BGB § 626 Nr. 247; 27. Januar 2011 – 2 AZR 825/09 – Rn. 29, BAGE 137, 54). Das unbefugte, vorsätzliche Löschen betrieblicher Daten auf EDV-Anlagen des Arbeitgebers ist ebenso wie das Vernichten von Verwaltungsvorgängen (vgl. LAG Hamm 2. Juni 2005 – 15 Sa 126/05 – juris) daher grundsätzlich als wichtiger Grund im Sinne des § 626 Abs. 1 BGB geeignet. Dabei kommt es nicht maßgeblich darauf an, ob sich der Arbeitnehmer durch das Löschen von Daten nach § 303a StGB oder § 303b StGB strafbar gemacht hat (vgl. dazu: OLG Nürnberg 23. Januar 2013 – 1 Ws 445/12 – ZD 2013, 282; aA Floeth EWiR 2013, 529; kritisch: Popp jurisPR-ITR 7/2013 Anm. 3) auch nicht darauf, ob und mit welchem Aufwand ein Teil dieser gelöschten Daten wieder hergestellt werden konnte oder darauf, ob und in welchem Umfang die Arbeitgeberin für den weiteren Geschäftsablauf diese Daten tatsächlich benötigte. Denn es gehört zu den vertraglichen Nebenpflichten eines Arbeitsverhältnisses im Sinne des § 241 Abs. 2 BGB, dass der Arbeitnehmer seinem Arbeitgeber den Zugriff auf betriebliche Dateien nicht verwehrt oder unmöglich macht (vgl. LAG Hessen 5. August 2013 – 7 Sa 1060/10 – Rn. 62, RDV 2014, 167; Ebert ArbRB 2014, 378, 379; zum Löschen eines Programms auf dem dienstlichen Rechner vgl. LAG Sachsen 17. Januar 2007 – 2 Sa 808/05 – Rn. 70 ff., LAGE KSchG § 1 Verhaltensbedingte Kündigung Nr. 96). Die sich aus § 241 Abs. 2 BGB ergebende Rücksichtnahmepflicht verlangt von den Parteien eines Arbeitsverhältnisses, gegenseitig auf die Rechtsgüter und Interessen der jeweils anderen Vertragspartei Rücksicht zu nehmen. Danach hat der Arbeitnehmer seine Verpflichtungen aus dem Arbeitsverhältnis so zu erfüllen und die in Zusammenhang mit dem Arbeitsverhältnis stehenden Interessen des Arbeitgebers so zu wahren, wie dies von ihm unter Berücksichtigung seiner Stellung im Betrieb, seiner eigenen Interessen und der Interessen der anderen Arbeitnehmer des Betriebs nach Treu und Glauben billigerweise verlangt werden kann (vgl. BAG 8. Mai 2014 – 2 AZR 249/13 – Rn. 19, aaO). Ein unbefugtes Löschen von dem Arbeitgeber zustehenden und an diesen in entsprechender Anwendung von § 667 BGB herauszugebenden Dateien stellt sich als erhebliche Pflichtverletzung dar. Dem Arbeitgeber steht ein Anspruch in entsprechender Anwendung von § 667 BGB auf Herausgabe der im Arbeitsverhältnis vom Arbeitnehmer erstellten oder von Dritten erlangten digitalen Unterlagen zu (vgl. MüKo-BGB/Schäfer 8. Aufl. § 667 Rn. 18; vgl. auch: Röckl NZA-RR 2016, 505). Nach § 667 BGB ist der Arbeitnehmer wie eine Beauftragter verpflichtet, dem Arbeitgeber alles, was er zur Ausführung der ihm übertragenen Arbeit erhalten und was er aus der Geschäftsbesorgung erlangt hat, herauszugeben. Diese auftragsrechtlichen Grundsätze finden auch bei Arbeitsverhältnissen Anwendung (vgl. BAG 21. August 2014 – 8 AZR 655/13 – Rn. 36, BAGE 149, 47; 14. Dezember 2011 – 10 AZR 283/10 – Rn. 17, AP BGB § 667 Nr. 2 = EzA BGB 2002 § 667 Nr. 2). Zur Ausführung der übertragenen Arbeit erhalten hat der Arbeitnehmer alles, was ihm zum Zwecke der Durchführung des Arbeitsverhältnisses vom Arbeitgeber zur Verfügung gestellt worden ist. Aus dem Arbeitsverhältnis erlangt ist jeder Vorteil, den der Arbeitnehmer aufgrund eines inneren Zusammenhangs mit dem Arbeitsverhältnis erhalten hat (vgl. BAG 21. August 2014 – 8 AZR 655/13 – aaO; 14. Dezember 2011 – 10 AZR 283/10 – Rn. 19, aaO mwN). Hierzu gehören Unterlagen, die dem Arbeitnehmer vom Arbeitgeber bzw. dessen Repräsentanten zur Verfügung gestellt worden sind (§ 667 Alt. 1 BGB), und die, die er während des Arbeitsverhältnisses, beispielsweise durch einen Schriftverkehr mit Dritten, erlangt hat (§ 667 Alt. 2 BGB). Aus der Geschäftstätigkeit iSd. § 667 BGB erlangt sind auch die vom Arbeitnehmer im Zusammenhang mit seiner Tätigkeit für den Arbeitgeber selbst angelegten Akten, sonstige Unterlagen und Dateien – mit Ausnahme von privaten Aufzeichnungen (vgl. BAG 14. Dezember 2011 – 10 AZR 283/10 – Rn. 20, aaO; vgl. auch: BAG 24. November 1960 – 5 AZR 261/60 – AP LitUrhG § 11 Nr. 1). Wenn ein Arbeitnehmer seinem Arbeitgeber eigenmächtig den Zugriff zu solchen Daten entzieht (vgl. zur Verwendung eines Sicherungsprogramms, welches die Zugriffsmöglichkeit für den Arbeitgeber verhinderte: LAG Mecklenburg-Vorpommern 18. Juli 2006 – 3 Sa 474/05 – juris) oder diese löscht, verstößt er derart gegen die selbstverständlichen Nebenpflichten eines jeden Arbeitnehmers, die Interessen des Arbeitgebers als seines Vertragspartners zu berücksichtigen, dass ein solches Verhalten in aller Regel zur sofortigen Beendigung des Arbeitsverhältnisses berechtigt und die Fortsetzung bis zum Ende der Kündigungsfrist unzumutbar ist (vgl. LAG Hamm 16. März 2016 – 15 Sa 451/15 – Rn. 100, juris; LAG Hamburg 24. Februar 2015 – 2 TaBV 10/14 – Rn. 44, juris; LAG Hessen 5. August 2013 – 7 Sa 1060/10 – RDV 2014, 167; LAG Köln 24. Juli 2002 – 8 Sa 266/02 – NZA-RR 2003, 303; Ebert, ArbRB 2014, 378). Einer Abmahnung bedarf es in der Regel nicht, da ein Arbeitnehmer üblicherweise nicht annehmen kann, das unbefugte Löschen von geschäftlichen Daten werde vom Arbeitgeber hingenommen werden (vgl. Ebert ArbRB 2014, 378, 381). Ob eine Verletzung arbeitsvertraglicher (Neben-)Pflichten vorliegt, entscheidet sich nach der objektiven Rechtslage. Handelt der Arbeitnehmer in der Annahme, sein Verhalten sei rechtmäßig, hat grundsätzlich er selbst das Risiko zu tragen, dass sich seine Rechtsauffassung als unzutreffend erweist (vgl. BAG 19. Januar 2016 – 2 AZR 449/15 – Rn. 29, AP BGB § 626 Nr. 257; 22. Oktober 2015 – 2 AZR 569/14 – Rn. 22, BAGE 153, 111).

(c) Der Kläger hat auch keinen – generellen – Rechtfertigungs- oder Entschuldigungsgrund substantiiert vorgetragen, der ihn berechtigte, Datenlöschungen vorzunehmen. Grundsätzlich stehen sämtliche Dateien in sämtlichen Stadien, dh. auch Entwurfsfassungen oder Vorkorrespondenzen dem Arbeitgeber zu; vorbereitende Unterlagen fallen unter § 667 BGB (vgl. MüKo-BGB/Schäfer § 667 Rn. 22). Der Kläger irrt, wenn er meint, er habe „seine" Dateien auf „seinem" Arbeitsplatz gelöscht. In diesem Zusammenhang ist es auch nicht Sache der Beklagten zu recherchieren und vorzutragen, ob und ggf. in welchem weiteren Verzeichnis auf dem Server sich frühere oder

spätere Versionen der Dateien oder ggf. Kopien befinden bzw. welche konkrete Personen in der Vergangenheit welche konkrete Dateien per E-Mail bereits erhalten haben, um einen Rechtfertigungsgrund auszuschließen. Vielmehr war es – im Sinne einer sekundären Darlegungslast – Sache des Klägers, den von ihm behaupteten Rechtfertigungsgrund für den komplett von ihm gelöschten Datenbestand vorzutragen, nachdem er den Löschvorgang ausgeführt und behauptet, für eine anderweitige Sicherung bzw. Speicherung und Verfügbarkeit des Datenbestands bei der Beklagten gesorgt zu haben. Das völlig pauschale Vorbringen des Klägers, er habe nur „aufgeräumt" und Dateien gelöscht, welche nicht relevant bzw. ohnehin an anderen Speicherorten bereits vorhanden seien, ist nicht geeignet, einen Rechtfertigungsgrund darzustellen und die Beklagte daraufhin zu veranlassen, dieses Vorbringen entkräften und einen Rechtfertigungsgrund ausschließen zu müssen.

Betriebsrat: Kommunikation in deutscher Sprache (Ls)

(**Landesarbeitsgericht Nürnberg**, Beschluss vom 18. Juni 2020 – 1 TaBV 33/19 –)

1. **Der Betriebsrat kann nicht verlangen, dass der Vertreter des Arbeitgebers in Gesprächen mit ihm – dem Betriebsrat – in deutscher Sprache spricht und diese versteht, wenn gewährleistet ist, dass jeweils entsprechende Übersetzungen erfolgen.**
2. **Existieren keine arbeitgeberseitigen Vorgaben zur Verwendung einer Sprache, kann der Betriebsrat ein Begehren dahingehend, dass der Arbeitgeber bzw. sein Filialleiter mit Mitarbeitern immer in deutscher Sprache kommunizieren muss, auch nicht auf den Grundsatzes der vertrauensvollen Zusammenarbeit des § 87 Abs. 1 Nr. 1 BetrVG stützen.**
3. **Entscheidend sei allein, dass die Erklärungen in deutscher Sprache beim Betriebsrat ankommen und von den Betriebsratsmitgliedern in deutscher Sprache abgegeben werden können – wie das passiert, ist dem Arbeitgeber überlassen. Es ist also nicht erforderlich, dass die Personalabteilung oder der Filialleiter selbst auf Deutsch kommunizieren (können).**

(Nicht amtliche Leitsätze)

Kein Sonderkündigungsschutz als DSB bei verabredeter, aber noch nicht vollzogener Benennung

(**Landesarbeitsgericht Niedersachsen**, Urteil vom 9. Juni 2020 – 9 Sa 608/19 –)

1. **Die Benennung eines Datenschutzbeauftragten erfordert zwar nicht die Schriftform, bedarf aber gleichwohl einer eindeutigen, uneingeschränkten Erklärung gegenüber der zu benennenden Person.**
2. **Demgemäß liegt eine Benennung i.S.d. Art. 37 DS-GVO nur dann vor, wenn nach dem Inhalt der Erklärung zur Benennung auch sämtliche Aufgaben, nebst der verbundenen Rechtsstellung eines Datenschutzbeauftragten, auch gegenüber der Aufsichtsbehörde übertragen werden sollen.**
3. **Eine zunächst „interne" Bestellung, die nach einer Einarbeitung später durch Mitteilung an die Aufsichtsbehörde „offiziell" werden soll, enthält keine wirksame Benennung. Eine Aufteilung in interne und externe Rechtsstellung des Datenschutzbeauftragten ist nicht möglich.**

(Nicht amtliche Leitsätze)

Sachverhalt:

Die Parteien streiten u.a. über die Benennung des Klägers als Datenschutzbeauftragter der Beklagten und über die Beendigung des Arbeitsverhältnisses.

Der Kläger war seit 01.01.2019 bei der Beklagten als Wirtschaftsjurist gem. Arbeitsvertrag beschäftigt. Im Zuge der Einstellungsgespräche am 28.11.2018 und 06.12.2018 sprachen die Parteien unter anderem darüber, dass der Kläger Datenschutzbeauftragter werden solle.

Das Amt des bei der Beklagten bestellten Datenschutzbeauftragten endete am 31.12.2018. Unmittelbar nach Beginn des Arbeitsverhältnisses wurde für den Kläger die Teilnahme an der Schulung TÜV-Nord zum Thema Datenschutzbeauftragter für den Zeitraum 11. bis 14.02.2019 gebucht. Die Mitarbeiter wurden darüber informiert, dass der Kläger „nach seiner Einarbeitung und Schulung offiziell die Rolle des Datenschutzbeauftragen übernehmen solle".

Am 16.01.2019 hörte die Beklagte durch Frau [Vorname, Nachname, Personalleiterin] den Betriebsrat zur beabsichtigten Probezeitkündigung an. Der Betriebsrat hat ausweislich des Anhörungsschreibens vom 16.01.2019 noch am selben Tag zugestimmt. Am 17.01.2019 erhielt der Kläger das Kündigungsschreiben vom 16.01.2019. Die Kündigung wurde zum 31.01.2019 erklärt. An der Fortbildung zum Datenschutzbeauftragten nahm der Kläger nicht mehr teil.

Der Kläger hat die Ansicht vertreten, er sei im Zeitpunkt der Kündigung bereits zum Datenschutzbeauftragten benannt worden. Schon bei den vor Abschluss des Arbeitsvertrages geführten Gesprächen sei ihm zugesagt worden, zum Datenschutzbeauftragten benannt zu werden. Ein anderer Datenschutzbeauftragter ab dem 01.01.2019 sei nicht, auch nicht vorübergehend, im Amt gewesen. Entgegen der Behauptung der Beklagten sei auch nicht Herr [Vorname Nachname, Mitarbeiter der IT-Abteilung] interimsweise zum Datenschutzbeauftragten ernannt worden. Vielmehr habe dieser ihm die Unterlagen des Datenschutzbeauftragten am 15.01.2019 ausgehändigt. Tatsächlich sei er auch mit Aufgaben des Datenschutzbeauftragten beschäftigt gewesen. Dies folge aus 21 Sachverhalten, wie im Schriftsatz vom 09.05.2019 ausgeführt. Aus der Mitteilung an alle Beschäftigten vom 09.01.2019 folge seine Benennung zum Datenschutzbeauftragten. Der Kläger hat außerdem die ordnungsgemäße Betriebsratsanhörung gerügt, insbesondere sei dem Betriebsrat nicht mitgeteilt worden, dass er Datenschutzbeauftragter sei.

Die Beklagte hat behauptet, dass der Kläger nicht Datenschutzbeauftragter gewesen sei. Es sei vielmehr darauf hingewiesen worden, dass der Kläger Datenschutzbeauftragter werden könne, wenn er die erforderliche Fortbildung absolviert und sich im Arbeitsverhältnis bewährt habe. Auch aus der Information der Geschäftsführung vom 09.01.2019 folge ebenfalls keine Benennung des Klägers zum Datenschutzbeauftragten. Vielmehr sei er als Ansprechpartner für Fragen im Zusammenhang mit dem Datenschutz benannt wor-

den. Das bedeute aber nicht, dass er die Rechtstellung des Datenschutzbeauftragten innehatte. Die Betriebsratsanhörung sei ordnungsgemäß erfolgt. Insbesondere sei dem Betriebsrat nicht mitzuteilen gewesen, dass der Kläger Datenschutzbeauftragter sei, weil dies nicht zutreffe.

Das Arbeitsgericht hat die Klage mit Urteil vom 26.06.2019 abgewiesen, weil der Kläger nicht zum Datenschutzbeauftragten benannt worden sei.

Aus den Gründen:

I. Der Kläger hat keinen Anspruch auf Feststellung, dass er Datenschutzbeauftragter der Beklagten ist.

1. Der Feststellungsantrag ist zulässig, weil er sich auf Feststellung des Bestehens oder Nichtbestehens eines Rechtsverhältnisses i.S.v. § 256 Abs. 1 ZPO bezieht. Da sich die Parteien um die Rechtstellung des Klägers zum Datenschutzbeauftragten streiten, besteht unzweifelhaft ein Feststellungsinteresse.

2. Der Kläger war seitens der Beklagten nicht zum Datenschutzbeauftragten während des Arbeitsverhältnisses benannt worden.

Nach Art. 37 Abs. 1 DS-GVO benennt der Verantwortliche unter den aufgeführten Voraussetzungen einen Datenschutzbeauftragten. § 38 BDSG bestimmt ergänzend zur Datenschutzgrundverordnung, dass eine Datenschutzbeauftragte oder ein Datenschutzbeauftragter zu benennen ist, soweit in der Regel mindestens 10 Personen ständig mit der automatisierten Verarbeitung personenbezogener Daten beschäftigt werden. Nach Art. 37 Abs. 5 DS-GVO wird der Datenschutzbeauftragte auf der Grundlage seiner beruflichen Qualifikation und insbesondere des Fachwissens benannt, das er auf dem Gebiet des Datenschutzrechts und der Datenschutzpraxis besitzt, sowie auf der Grundlage seiner Fähigkeit zur Erfüllung der in Art. 39 DS-GVO genannten Aufgaben. Nach Art. 37 Abs. 6 DS-GVO kann der Datenschutzbeauftragte Beschäftigter des Verantwortlichen sein oder seine Aufgaben auf der Grundlage eines Dienstleistungsvertrages erfüllen. Nach Art. 37 Abs. 7 DS-GVO veröffentlicht der Verantwortliche die Kontaktdaten des Datenschutzbeauftragten und teilt diese der Aufsichtsbehörde mit. Der Aufgabenkatalog des Datenschutzbeauftragten richtet sich nach Art. 39 DS-GVO. Weder die Datenschutzgrundverordnung noch das Bundesdatenschutzgesetz stellen zusätzliche Anforderungen an das „Benennen" der Datenschutzbeauftragten oder des Datenschutzbeauftragten. Insbesondere ist entgegen der früheren Fassung des Bundesdatenschutzgesetzes keine Schriftform für die Benennung erforderlich. Dass die Beklagte verpflichtet war, eine Datenschutzbeauftragte oder einen Datenschutzbeauftragten zu benennen, ist zwischen den Parteien unstreitig. Die Voraussetzungen von Art. 37 Abs. 1 Ziff. b u. c DS-GVO und § 38 BDSG liegen unstreitig vor.

2. Keiner der vom Kläger behaupteten Tatbestände ist geeignet, eine Benennung im Sinne von Art. 37 Abs. 1 DS-GVO, § 38 BDSG darzustellen. Nach dem Wortlaut erfordert „Benennen" eines Datenschutzbeauftragten, dass eine Person als Datenschutzbeauftragter bezeichnet wird. Mit dem Benennen wird die Position individualisiert und einer bestimmten Person oder Stelle zugeschrieben. Da die Datenschutzgrundverordnung unmittelbar geltendes Recht ist, richtet sich die Benennung des Datenschutzbeauftragten zunächst nach Art. 37 DS-GVO, wobei Art. 37 Abs. 1 Ziff. b DS-GVO offen lässt, wann eine umfangreiche regelmäßige und systematische Überwachung von betroffenen Personen eine Benennung erforderlich machen. In § 38 BDSG ist lediglich eine weitere Konkretisierung der Voraussetzungen erfolgt. Bei der Benennung des Datenschutzbeauftragten ist zwischen dem Bestellungsvorgang und dem zugrundliegenden Rechtsverhältnis zu trennen, wie aus Art. 37 Abs. 6 DS-GVO folgt. Voraussetzung für die Benennung ist nicht, dass eine bestimmte Qualifikation oder Fortbildung vorliegt oder absolviert wurde. Allerdings geht Art. 37 DS-GVO davon aus, dass der Benannte ein gewisses Fachwissen hat, um die Aufgaben erfüllen zu können.

Mit der Benennung des Datenschutzbeauftragten ist gem. Art. 38 DS-GVO die dort beschriebene Stellung des Datenschutzbeauftragten verbunden. Danach besteht ein Benachteiligungsverbot; insbesondere ist der Datenschutzbeauftragte weisungsfrei (Art. 38 Abs. 3 DS-GVO). Aus der Zusammenschau von Art. 37 bis 39 DS-GVO folgt, dass mit der Benennung ohne weiteres die beschriebene Rechtstellung des Datenschutzbeauftragten eintritt und ihm auch uneingeschränkt alle Aufgaben nach Art. 39 DS-GVO obliegen. § 6 Abs. 4 BDSG ergänzt zusätzlich die Rechtstellung des Datenschutzbeauftragten im Rahmen eines Arbeitsverhältnisses um den Sonderkündigungsschutz. Insbesondere aus der Zusammenschau von Art. 37 und Art. 39 DS-GVO folgt aber auch, dass mit der Benennung die Aufgaben des Datenschutzbeauftragten insgesamt anfallen. Neben der Unterrichtung und Beratung des Verantwortlichen fallen insbesondere Überwachungsaufgaben und auch die Zusammenarbeit mit der Aufsichtsbehörde sowie Tätigkeit als Anlaufstelle für die Aufsichtsbehörde an. Auch wenn die Mitteilung der Kontaktdaten an die Aufsichtsbehörde nach Art. 37 Abs. 6 DS-GVO nicht Voraussetzungen für die Benennung sind, ergibt sich aus der Zusammenschau aber, dass eine Trennung zwischen internem und externem Datenschutzbeauftragten von der Datenschutzgrundverordnung und auch vom Bundesdatenschutzgesetz nicht vorgesehen ist. Das bedeutet, dass eine Benennung i.S.v. Art. 37 DS-GVO nur dann vorliegt, wenn nach dem Inhalt der Erklärung zum Benennen auch sämtliche Aufgaben mit der damit verbundenen Rechtstellung eines Datenschutzbeauftragten, auch gegenüber der Aufsichtsbehörde übertragen werden sollen. Eine Aufteilung in interne und externe Rechtsstellung des Datenschutzbeauftragten ist nicht vorgesehen.

3. Gemessen daran ist der Kläger nicht zum Datenschutzbeauftragten benannt worden.

a. Mit dem Abschluss des Arbeitsvertrages am 18.12.2018 war zwischen den Parteien keine Benennung zum Datenschutzbeauftragten verbunden. Der Arbeitsvertrag nennt an keiner Stelle, dass der Kläger zum Datenschutzbeauftragten ab 01.01.2019 benannt wird. Es kann dahinstehen, welche konkreten Zusagen gegenüber dem Kläger in den Vorgesprächen am 28.11. und 06.12.2018 erfolgt sind. Unstreitig haben die Parteien darüber gesprochen, dass der Kläger Datenschutzbeauftragter werden soll. Der Inhalt des Arbeitsvertrages spricht dagegen, dass bereits zum 01.01.2019 die Benennung zum Datenschutzbeauftragten erfolgt sein soll. Letztendlich behauptet auch der Kläger das nicht, zumal aus dem von der Beklagten vorgelegten EMail-Verkehr vom 07.01.2019 (Bl. 56 bis 57 Rs, Anl. B6 zum Schriftsatz vom 10.04.2019) folgt, dass der Kläger selbst bis zu diesem Zeitpunkt nicht davon ausgegangen ist, Datenschutzbeauftragter zu sein.

b. Ob dem Kläger seitens Herrn [Nachname, IT-Leiter] am 08.01.2019 im Rahmen der Gespräche über die Neuorganisation des Datenschutzes gesagt wurde, er werde zum Datenschutzbeauftragten benannt, kann ebenfalls dahinstehen. Im Laufe der mündlichen Verhandlung hat sich herausgestellt, dass entgegen der Behauptung des Klägers im Schriftsatz vom 09.10.2019 Herr

[Vorname Nachname, IT-Leiter = späterer Prokurist] nicht Prokurist und auch sonst nicht ersichtlich war, dass er zur Abgabe einer solchen Erklärung befugt war. Darüber hinaus bliebe bei dieser in die Zukunft gerichtete Äußerung immer noch offen, zu welchem Zeitpunkt der Kläger Datenschutzbeauftragter werden soll. Allein in der Gesamtschau mit der am Folgetag erfolgten Information durch die Geschäftsführung hätte möglicherweise ein anderer Schluss gezogen werden können. Die Benennung zum Datenschutzbeauftragten erfolgt durch die Geschäftsführung oder in ihrem Auftrag und nicht durch einen nicht bevollmächtigten Mitarbeiter.

c. Die Mitteilung vom 09.01.2019 lässt ebenfalls nicht den Schluss zu, dass der Kläger zum Datenschutzbeauftragten benannt wurde. Die Mitteilung stellt weder selbst eine Benennung dar, noch nimmt sie Bezug auf eine vorangegangene Benennung. Das ergibt die Auslegung der Information. Dem Kläger ist zuzugestehen, dass die Überschrift der Mitteilung zunächst auf eine Benennung zum Datenschutzbeauftragten schließen lassen könnte. Und zwar rückwirkend zum 01.01.2019. Der Inhalt der Mitteilung ergibt aber nicht, dass der Kläger zum Datenschutzbeauftragten benannt wurde. Der Inhalt der Mitteilung verweist auf die vorgenommene organisatorische Veränderung und Neuzuordnung der Rolle des Datenschutzbeauftragten zu Legal im Bereich C. Aus dieser Mitteilung folgt nicht, dass der Kläger bereits zum 01.01.2019 zum Datenschutzbeauftragten benannt, sondern lediglich, dass organisatorisch die Position des Datenschutzbeauftragten verlagert wurde. Die Gründe dafür werden im Folgesatz erläutert. Sodann wird der Kläger ab sofort als Ansprechpartner für Fragen im Zusammenhang mit dem Datenschutz bezeichnet. Die Information wählt nicht den Begriff Datenschutzbeauftragten, sondern den Begriff des Ansprechpartners. Hier wird der Zeitpunkt mit „ab sofort" bezeichnet und nicht rückwirkend. Der Kläger ist Mitarbeiter in der Rechtsabteilung, und die Beklagte hat hierzu darauf verwiesen, dass Datenschutzfragen nicht allein vom Datenschutzbeauftragten bearbeitet werden, sondern auf der Ebene der Sachbearbeitung auch durch entsprechende Mitarbeiter. Dafür spricht auch der Aufgabenkatalog von Art. 39 DS-GVO, wonach der Datenschutzbeauftragte gerade nicht im Auftrag des Arbeitgebers als Verantwortlicher tätig wird und prüft, sondern lediglich beratend, unterrichtend und überwachend tätig wird, und dies zudem weisungsfrei (Art. 38 Abs. 3 DS-GVO). Angesichts der Fülle von datenschutzrechtlichen Fragen, die im Zusammenhang mit nahezu jeder Aufgabe auftreten können, ist es nachvollziehbar, dass nicht nur der Datenschutzbeauftragte mit datenschutzrechtlichen Sachverhalten konfrontiert wird, sondern je nach Größe und Gegenstand des Unternehmens eine entsprechende Anzahl weiterer Mitarbeiter. Daher ist es unerheblich, dass nach dem klägerischen Vortrag zahlreiche datenschutzrechtliche Sachverhalte zu bearbeiten waren. Die Mitteilung, dass der Kläger Ansprechpartner für Fragen im Zusammenhang mit dem Datenschutz ist, ist damit letztendlich die Mitteilung einer (geänderten) Geschäftsverteilung. Im Folgesatz wird dann in die Zukunft gerichtet angekündigt, dass der Kläger die Rolle des Da-tenschutzbeauftragten erst nach seiner Einarbeitung und Schulung übernehmen soll. Die Benennung des Datenschutzbeauftragten steht damit unter zwei Bedingungen. Auch aus dem Wortlaut „offiziell" folgt nichts anderes. Die Benennung des Datenschutzbeauftragten kann nur insgesamt erfolgen; und zwar verbunden mit allen Konsequenzen hinsichtlich der Benennung und Aufgabenübertragung des Datenschutzbeauftragten. Daran ändert auch der Umstand nichts, dass die Beklagte ab dem 01.01.2019 keine andere Person zum Datenschutzbeauftragten benannt hatte.

d. Da es sich bei der Information durch die Geschäftsführung nicht um eine Willenserklärung, sondern eine Wissensmitteilung handelt, kommt auch eine AGB-Kontrolle nicht in Betracht. Die Mitteilung vom 09.01.2019 ist keine Vertragsbedingung im Sinne von § 305 Abs. 1 BGB; selbst wenn, ergeben sich aus o.g. Auslegung keine Zweifel daran, dass der Kläger nicht zum Datenschutzbeauftragten benannt wurde.

II. Das Arbeitsgericht hat zurecht festgestellt, dass das Arbeitsverhältnis durch die Kündigung vom 16.01.2019, zugegangen am 17.01.2019 mit Ablauf des 31.01.2019 beendet wurde.

1. Gem. Ziff. VIII 1 u. 2 des Ergänzungsvertrages zum Arbeitsvertrag vom 18.12.2018, kann das Arbeitsverhältnis innerhalb der Probezeit mit einer zweiwöchigen Kündigungsfrist gekündigt werden. Diese Frist ist eingehalten.

2. Da der Kläger nicht Datenschutzbeauftragter bei der Beklagten war, steht der Kündigung gem. § 6 Abs. 4 S. 2 BDSG nicht entgegen. Die Stellung des Datenschutzbeauftragten ist nicht Inhalt des Arbeitsverhältnisses geworden, weder nach dem schriftlichen Arbeitsvertrag, noch durch eine spätere Erklärung.

Die Kündigung ist auch nicht nach § 102 Abs. 1 BetrVG unwirksam (wird ausgeführt).

Fotos auf Fanpage bei Facebook (Ls)

(**Oberverwaltungsgericht Lüneburg**, Beschluss vom 19. Januar 2021 – 11 LA 16/20 –)

1. **Die Veröffentlichung eines Fotos auf einer Fanpage bei Facebook, auf dem Personen identifizierbar sind, stellt eine Verarbeitung personenbezogener Daten dar, die einer Legitimation nach datenschutzrechtlichen Vorschriften bedarf.**

2. **Kann das Ziel einer Datenverarbeitung auch durch die Veröffentlichung anonymisierter Daten erreicht werden, ist eine unanonymisierte Veröffentlichung nicht erforderlich.**

3. **Bei einem auf einer Fanpage bei Facebook veröffentlichten Foto, auf dem Personen identifizierbar sind, die in die Veröffentlichung nicht eingewilligt haben, ist im Rahmen der Interessenabwägung nach Art. 6 Abs. 1 lit. f DS-GVO zugunsten der betroffenen Personen u.a. zu berücksichtigen, dass eine solche Veröffentlichung aufgrund bestehender Missbrauchsmöglichkeiten sowie aufgrund der großen Reichweite derartiger Netzwerke mit erheblichen Risiken verbunden ist.**

4. **Art. 21 GG, § 1 ParteienG stellen keine spezifischen Rechtsgrundlagen zur Verarbeitung personenbezogener Daten i.S.v. Art. 6 Abs. 1 lit. e, Abs. 2 und Abs. 3 DS-GVO dar.**

5. **Zur Frage, wann eine Datenverarbeitung zur journalistischen Zwecken i.S.d. Art. 85 Abs. 2 DS-GVO vorliegt.**

Einsicht in Bauunterlagen betrifft personenbezogene Daten des Grundstückseigentümers (Ls)

(**Verwaltungsgerichtshof Baden-Württemberg**, Urteil vom 17. Dezember 2020 – 10 S 3000/18 –)

1. **Ein auf § 1 Abs. 2 LIFG gestütztes Informationsbegehren auf Einsicht in die Bauakten des Nachbargrundstücks, soweit diese Angaben zur Statik des Gebäudes enthalten, betrifft im Sinne des Art.s 4 Nr. 1 DS-GVO personenbezogene Daten der betroffenen Eigentümer des Nachbargrundstücks.**
2. **Bei der Abwägung nach § 5 Abs. 1 LIFG müssen die im Einzelfall kollidierenden Interessen identifiziert und konkretisiert sowie gewichtet und zueinander ins Verhältnis gesetzt werden; die behördliche Abwägungsentscheidung ist gerichtlich voll überprüfbar.**
3. **Der Gesetzgeber hat in § 5 Abs. 1 LIFG dem Datenschutz einen relativen Vorrang eingeräumt; zu dessen Überwindung muss das öffentliche Informationsinteresse überwiegen.**
4. **Für ein überwiegendes öffentliches Informationsinteresse im Sinne des § 5 Abs. 1 LIFG an der ausnahmsweise zulässigen Offenbarung der an sich geschützten personenbezogenen Informationen genügt grundsätzlich weder das allgemeine, in § 1 Abs. 1 LIFG ausgedrückte öffentliche Interesse an einem „freien Zugang zu amtlichen Informationen", noch das generelle (vom jeweiligen Einzelfall unabhängige) Interesse an einer öffentlichen Kontrolle der Gesetzmäßigkeit der Verwaltung.**
5. **Ist im Einzelfall das schutzwürdige Interesse der Betroffenen an einem Ausschluss des Zugangs zu ihren personenbezogenen Daten als sehr gering zu bewerten, so kann von einem überwiegenden öffentlichen Informationsinteresse ausgegangen werden, wenn Verdachtsmomente oder Unsicherheiten im Hinblick auf eine mögliche polizeiliche Gefahr vorliegen, die eine Aufklärung des Sachverhalts unter Berücksichtigung der begehrten Informationen als vernünftig erscheinen lassen.**

Kein Schadensersatzanspruch wegen Datenschutzverletzung (Ls)

(**Landgericht Hamburg**, Urteil vom 4. September 2020 – 324 S 9/19 –)

1. **Es führt nicht jeder Verstoß gegen die DS-GVO zu einer Ausgleichspflicht, denn der Verpflichtung zum Ausgleich eines immateriellen Schadens muss eine benennbare und insoweit tatsächliche Persönlichkeitsverletzung gegenüberstehen.**
2. **Werden die Daten durch die Erfassung im Terminformular seiner Webseite verarbeitet und durch die öffentliche Freischaltung auch verbreitet, handelt es sich um einen Vorfall von geringem Umfang und nicht erheblicher Bedeutung.**

Pflicht zum Tragen einer Mund-Nasen-Maske am Arbeitsplatz (Ls)

(**Arbeitsgericht Berlin**, Urteil vom 15. Oktober 2020 – 42 Ga 13034/20 –)

1. **Der Arbeitgeber ist verpflichtet, seine Beschäftigten und das Publikum vor Infektionen zu schützen.**
2. **Demgemäß kann eine Flugsicherheitsassistentin am Flughafen zum Tragen eines vom Arbeitgeber bereitgestellten Mund-Nasen-Schutzes angewiesen werden. Ein von der Arbeitnehmerin vorgeschlagenes Gesichtsvisier ist für den Schutz Dritter weniger geeignet als der beim Arbeitgeber vorgeschriebene Mund-Nasen-Schutz.**
3. **Dass Gründe vorliegen, nach denen das Tragen der Mund-Nasen-Maske aus gesundheitlichen Gründen nicht zumutbar ist, muss die Beschäftigte glaubhaft machen.**

(Nicht amtlicher Leitstz)

Homeoffice statt Änderungskündigung (Ls)

(**Arbeitsgericht Berlin,** Urteil vom 10. August 2020 – 19 Ca 13189/19 –)

Bevor der Arbeitgeber z.B. coronabedingt eine Änderungskündigung zur Zuweisung eines anderen Arbeitsbereiches ausspricht, hat er zu prüfen, ob die bisherige Arbeit, bei vorhandenen technischen Möglichkeiten, von zu Hause aus erledigt werden kann.

(Nicht amtlicher Leitsatz)

Keine Mitbestimmung bei Einsatz von „Greetern" (Ls)

(**Arbeitsgericht Berlin**, Beschluss vom 30. Juli 2020 – 4 BVGa 9401/20 –)

Bei der Einteilung von Beschäftigten als „Greeter", die unter anderem dafür zuständig sind, die Einhaltung der zulässigen Maximalzahl an Kunden in den Räumlichkeiten zu überwachen und durchzusetzen und die Kunden auf die Verpflichtung des Tragens einer Mund-Nasen-Bedeckung in den Räumlichkeiten sowie die Verwendung des bereitgestellten Desinfektionsschutzmittels hinzuweisen, handelt es sich um keine dem Mitbestimmungsrecht des Betriebsrats nach § 87 Abs. 1 Nr. 1 BetrVG unterliegende Maßnahme.

(Nicht amtlicher Leitsatz)

Praxisfälle, Informationen, Sonstiges

Aus den aktuellen Berichten und Informationen der Aufsichtsbehörden (52): Einzelfälle zum Beschäftigtendatenschutz im 28. TB des LfDI Rheinland-Pfalz vom 12.01.2021

Zusammengestellt und erläutert von Prof. Peter Gola*

In Kapitel 7 seines das Jahr 2019 betreffenden 28. Tätigkeitsbericht beschäftigt sich der LfDI Rheinland-Pfalz u.a. mit folgenden Fragen des Beschäftigtendatenschutzes

I. Die Amtsträgertheorie und ihre Grenzen/ Veröffentlichung von Funktionsträgern mit Außenkontakt

Dabei zeigt er auf, dass auch nach Inkrafttreten der DS-GVO die sog. Amtsträgertheorie anwendbar bleibt, wonach es einem Arbeitgeber oder Dienstherrn gestattet ist, im Rahmen seines Organisationsermessen darüber zu entscheiden, wie er sein Unternehmen oder seine Behörde nach außen darstellen möchte. In diesem Zusammenhang stehe es ihm grundsätzlich auch frei, die Namen und die dienstlichen Erreichbarkeiten seiner Beschäftigten zu veröffentlichen. Die Veröffentlichung ist aber auf die dienstlichen Erreichbarkeiten, also die dienstlichen Telefonnummern und E-Mail-Adressen, zu beschränken. Weitergehende Daten, wie beispielsweise Fotografien der Beschäftigten, dürfen nur auf Grundlage einer Einwilligung der Beschäftigten veröffentlicht werden. Außerdem ist es ausreichend, lediglich die Daten derjenigen Beschäftigten zu veröffentlichen, deren Tätigkeit typischerweise einen Kunden- oder Bürgerkontakt mit sich bringt. Nicht darunter fallen beispielsweise Personen, die im Archiv, der Registratur, dem Botendienst oder in der internen Buchhaltung beschäftigt sind.

Im Übrigen entbindet die Anwendung der Amtsträgertheorie den Arbeitgeber oder Dienstherren nicht von seiner Fürsorgepflicht. So kann es in besonderen Fällen angezeigt sein, auf die Veröffentlichung von Beschäftigtendaten gänzlich zu verzichten (z.B. bei Stalkingopfern).

II. Kennzeichnung von Justizvollzugsbeamten durch bebilderte Namensschilder

Die Strafvollzugsbediensteten des Justizvollzugs im Land Rheinland-Pfalz müssen an ihrer Dienstkleidung ein Namensschild mit einem Bild tragen. Hiergegen hatte sich ein Justizvollzugsbeamter gewandt, weil es häufiger vorkomme, dass Bedienstete und deren Familien von Gefangenen bedroht würden. Anhand der Namen der Bediensteten sei es über Profilsuchen im Internet schnell möglich, beispielsweise über Social-Media-Plattformen oder Anfragen bei Meldebehörden, Erkenntnisse über die Bediensteten selbst oder auch deren Familien zu erlangen.

Der LfDI ließ diesen allgemeinen Einwand jedoch nicht gelten. Er rechtfertigt das Erfordernis eines Namensschildes mit § 2 S. 2, 3 Abs. 1 Landesjustizvollzugsgesetz bzw. § 2 Landessicherungsverwahrungsvollzugsgesetz, wonach die Sicherstellung des Verbleibs der Gefangenen in den Einrichtungen gesetzliche Aufgabe des Justizvollzugsbeamten ist. Das Tragen von Namensschildern mit Fotografien durch Justizvollzugsbedienstete innerhalb der Einrichtung ist zur Erfüllung dieser Aufgabe erforderlich. So ist beispielsweise denkbar, dass sich Gefangene Zugang zu Dienstkleidung verschaffen und versuchen können, als Justizvollzugsbedienstete gekleidet die Anstalt zu verlassen. Durch einen Abgleich des Namens und der Fotografie auf dem Namensschild mit der tatsächlichen Trägerin oder dem Träger können diese versuchten Täuschungen aufgedeckt und ein Entweichen von Gefangenen aus dem Justizvollzug verhindert werden. Die Verwendung einer Dienstnummer oder einer pseudonymen Kennzeichnung sei für diese Zwecke nicht geeignet, da der Dienstherr der Erfüllung seiner gesetzlich zugewiesenen Aufgabe, nämlich die Gewährleistung der öffentlichen Sicherheit und Ordnung, nur noch mit einem unverhältnismäßigen Aufwand Rechnung tragen könnte. Die Identifizierung eines als Justizvollzugsbediensteter getarnten Gefangenen würde erheblich erschwert. Insbesondere in größeren Einrichtungen kann nicht sichergestellt werden, dass sich die Bediensteten untereinander persönlich kennen und so einen Täuschungsversuch unmittelbar aufdecken könnten.

III. Übermittlung von personenbezogenen Gehaltsabrechnungen im Rahmen von Förderprojekten

Wiederholt hatte sich der LfDI mit der Frage zu beschäftigten, ob im Rahmen der Bereitstellung von Fördermitteln durch Ministerien die die Bewilligung vornehmende nachgeordnete Behörde die Vorlage von Gehaltsnachweisen des aus den Fördermitteln finanzierten Personals verlangen darf. Dazu verweist er zunächst auf folgende Rechtslage: „Gemäß § 23 der Landeshaushaltsordnung (LHO) dürfen Ausgaben und Verpflichtungsermächtigungen für Leistungen an Stellen außerhalb der Landesverwaltung zur Erfüllung bestimmter Zwecke (Zuwendungen) veranschlagt werden, wenn das Land an der Erfüllung durch solche Stellen

* Der Autor ist Ehrenvorsitzender der Gesellschaft für Datenschutz und Datensicherheit e.V., Bonn.

ein erhebliches Interesse hat, das ohne die Zuwendungen nicht im notwendigen Umfang befriedigt werden kann. In diesem Zusammenhang normiert § 44 Abs. 1 LHO, dass zu bestimmen ist, wie die zweckentsprechende Verwendung der Zuwendungen nachzuweisen ist.

Hierzu wurden Regelungen in der Anlage der Verwaltungsvorschrift zum Vollzug der Landeshaushaltsordnung (VV-LHO) getroffen. Gemäß Ziffer 1.3 der allgemeinen Nebenbestimmungen für Zuwendungen zur Projektförderung (ANBest-P), die zum Bestandteil der Bewilligungsbescheide zumachen sind, ist anlässlich der Prüfung des Antrags auf Förderung unter anderem zu prüfen, ob der Zuwendungsempfänger seine Beschäftigten finanziell nicht besser stellt als vergleichbare Landesbedienstete. Höhere Vergütungen als nach dem TV-L bzw. dem TVöD sowie sonstige über- und außertarifliche Leistungen dürfen nicht gewährt werden. Um die Einhaltung dieser Nebenbestimmungen prüfen zu können, ist regelmäßig die Vorlage eines Gehaltsnachweises erforderlich, aus dem neben der Entgeltgruppe und der Entgeltstufe alle weiteren Bestandteile der Vergütung (wie z.B. Jahressonderzahlungen, Leistungsprämien, Bonuszahlungen, vermögenswirksame Leistungen etc.) hervorgehen, um diese für die Vergleichsberechnung zur Prüfung des Besserstellungsverbotes aus Ziffer 1.3 ANBest-P heranzuziehen. Um eine Vergleichsberechnung zur Prüfung des Besserstellungsverbotes aus Ziffer 1.3 ANBest-P durchführen zu können, sind in Zusammenhang mit Personalkosten u.a. die Eingruppierung (Entgeltgruppe und Entgeltstufe) der eingesetzten Personen sowie der entsprechende Arbeitsanteil, zu dem diese im Projekt tätig sind, anzugeben. Die Personalkosten selbst umfassen den Bruttoarbeitslohn zuzüglich der Arbeitgeberanteile zur Sozialversicherung. Darüber hinausgehende Angaben in den Gehaltsnachweisen (z.B. Familienstand und Konfession) können hingegen unkenntlich gemacht werden." Im Ergebnis kommt er zu dem Schluss, dass die Vorlage einer anonymisierten Gehaltsabrechnung nicht genüge, da ansonsten nicht sichergestellt werden könne, dass nur diejenigen aus den Zuwendungen bezahlt werden, welche in dem mit den Zuwendungen finanzierten Projekt tätig sind.

IV. Verarbeitung biometrischer Daten im Beschäftigtenverhältnis

Nicht hinnehmen müssen es nach Ansicht des LfDI Beschäftigte, dass der Arbeitgeber den Zugang zum dienstlichen Rechner durch biometrische Daten, in diesem Fall einen Fingerabdruck der Beschäftigten, absichert. Dies begründet er wie folgt: „Bei biometrischen Daten handelt es sich um besondere Kategorien personenbezogener Daten im Sinne des Art. 9 DS-GVO. Die Verarbeitung solcher Daten in einem Beschäftigungsverhältnis ist gemäß § 26 Abs. 3 BDSG nur zulässig, wenn dies zur Ausübung von Rechten oder zur Erfüllung rechtlicher Pflichten aus dem Arbeitsrecht, dem Recht der sozialen Sicherheit und des Sozialschutzes erforderlich ist und kein Grund zu der Annahme besteht, dass das schutzwürdige Interesse der betroffenen Person an dem Ausschluss der Verarbeitung überwiegt. Bei dieser Norm handelt es sich um eine abschließende Regelung, sodass für darüber hinausgehende Verarbeitungsszenarien in einem Beschäftigungsverhältnis nur Raum bleibt, wenn diese explizit gestattet werden. Dies ist beispielsweise mit der Regelung von § 22 Abs. 1 Nr. 1 lit. b BDSG der Fall, welcher die Verarbeitung besonderer Kategorien personenbezogener Daten zur Beurteilung der Arbeitsfähigkeit von Beschäftigten erlaubt. Die in den entsprechenden spezialgesetzlichen Erlaubnistatbeständen in den Blick genommenen Kategorien besonderer personenbezogener Daten dürften derweil in erster Linie Gesundheitsdaten sein. Die Verarbeitung biometrischer Daten im Beschäftigungsverhältnis dürfte nur in den allerwenigsten Fällen angezeigt sein. Denkbar wäre dies beispielsweise bei Personen, die in sicherheitssensiblen Bereichen, wie z.B. klassifizierten Forschungsprojekten oder militärischen Einrichtungen, beschäftigt sind. Hier könnte ein Interesse daran bestehen, den Zugang zu Bereichen oder Informationen durch einen zusätzlichen Faktor, wie eben ein biometrisches Merkmal, abzusichern. Bei einer gewöhnlichen Tätigkeit besteht dieses Bedürfnis hingegen nicht, weshalb die Zulässigkeit einer derartigen Verarbeitung biometrischer Daten nicht gegeben ist." Sodann verweist er auf eine Entscheidung des Arbeitsgerichts Berlin (Urt. v. 16.10.2019 (Az. 29 Ca 5451/19 = RDV 2020), nach der eine Zeiterfassung per Fingerabdruck nicht ohne freiwillige Einwilligung der Beschäftigten erfolgen darf.

V. Zulässigkeit anlassloser Anti-Terror-Mitarbeiterscreenings

Aufgrund der EU-Antiterror-Verordnungen und der darin enthaltenen Bereitstellungsverboten sehen sich viele Unternehmen dazu gezwungen, anlasslose Anti-Terror-Mitarbeiterscreenings durchzuführen und ihre Beschäftigten turnusmäßig mit den Namenslisten der entsprechenden Verordnungen abzugleichen. Einerseits geschieht dies aus Angst vor Sanktionen nach dem Außenwirtschaftsgesetz (AWG), andererseits, um den Status eines „zugelassenen Wirtschaftsbeteiligten" zu erhalten bzw. aufrecht zu erhalten. Mit der Zulässigkeit dieser Vorgehensweise hat sich der LfDI anlässlich einer Anfrage der Industrie- und Handelskammer auseinandergesetzt: „Zunächst ist anzumerken, dass die Anti-Terror-Verordnungen selbst keine Regelungen bezüglich der Verarbeitung von personenbezogenen Daten im Rahmen von Mitarbeiterscreenings enthalten. Sie ordnen lediglich an, dass den in einschlägigen Listen genannten natürlichen und juristischen Personen sowie Organisationen keine wirtschaftlichen Ressourcen bereitgestellt und ihnen gegenüber keine Leistungen erbracht werden dürfen. Dies schließt auch die Auszahlung von Lohn, Gehalt oder anderen vermögenswirksamen Leistungen ein (Bereitstellungsverbot).

Die einschlägige Rechtsgrundlage für anlasslose Anti-Terror-Mitarbeiterscreenings ist § 26 Abs. 1 S. 1 Bundesdatenschutzgesetz (BDSG). Dieser normiert, dass personenbezogene Daten von Beschäftigten für Zwecke des Beschäftigungsverhältnisses unter anderem dann verarbeitet werden dürfen, wenn dies für die Begründung eines Beschäftigungsverhältnisses oder nach Begründung des Beschäftigungsverhältnisses für dessen Durchführung erforderlich ist. Zu diesen Zwe-

cken gehören auch regelmäßige Entgeltzahlungen an Beschäftigte.

Anlasslose Listenabgleiche aufgrund dieser Rechtsgrundlage sind jedoch nur dann zulässig, wenn sie auch im Rahmen dieses Zweckes erforderlich sind. Eine Erforderlichkeit ist immer dann gegeben, wenn die personenbezogenen Daten für die Aufgabenerfüllung des Verantwortlichen unabdingbar sind. Dies ist wiederum der Fall, wenn die Aufgabe ohne die Kenntnis der Information nicht, nicht rechtzeitig, nur mit unverhältnismäßigem Aufwand oder nur mit sonstigen unverhältnismäßigen Nachteilen erfüllt werden kann. Einen solchen unverhältnismäßigen Nachteil für den Fall, dass ein Listenabgleich nicht erfolgt, stellen die in den Straf- und Bußgeldvorschriften des AWG in Aussicht gestellten Sanktionen bei Zuwiderhandlung dar. Die Höhe dieser Sanktionen hängt davon ab, ob von einer vorsätzlichen oder fahrlässigen Verwirklichung eines entsprechenden Bußgeldtatbestandes ausgegangen wird. Vorsatz setzt voraus, dass der Arbeitgeber Kenntnis davon hat, dass einer seiner Mitarbeiter auf einschlägigen Listen geführt wird. Für die Beurteilung des Merkmals der Fahrlässigkeit ist auf die Kenntnis des Arbeitgebers bezüglich der Möglichkeit des Eintritts der Tatbestandsverwirklichung abzustellen.

Es ist somit zu fragen, in welchem Maße der Arbeitgeber auf die anlasslosen Anti-Terror-Mitarbeiterscreenings angewiesen ist, um die Möglichkeit der Tatbestandsverwirklichung überhaupt zu erkennen. Dieses dürfte in kleinen und mittelgroßen Betrieben, in welchem der Geschäftsführer oder sonstige vertretungsberechtigte Organe dazu in der Lage sind, das Verhalten ihrer Mitarbeiter zu beobachten und daraus Schlüsse auf eine mögliche Zugehörigkeit zu terroristischen Netzwerken zu schließen, eher gering sein.

In Großkonzernen hingegen, die von einer diffizilen und schwer überblickbaren Unternehmensstruktur geprägt sind, dürften regelmäßige Screenings die einzige Möglichkeit für die im Sinne des AWG Verantwortlichen sein, den Vorwurf der fahrlässigen Begehungsweise entfallen zu lassen, da ihnen aufgrund der Tatsache, dass sie unmöglich jeden einzelnen Mitarbeiter persönlich kennen können, keine anderen Anhaltspunkte zur Verfügung stehen, um die möglicherweise bestehende Zugehörigkeit zu terroristischen Netzwerken beurteilen zu können. Die Erforderlichkeit der Verarbeitung von Beschäftigtendaten in Form eines Listenabgleichs kann also nicht für alle Unternehmen einheitlich beantwortet werden, sondern hängt maßgeblich von der Unternehmensstruktur ab.

Ähnlich verhält es sich auch mit dem Abgleich der Anti-Terror-Listen zur Erlangung oder Aufrechterhaltung des Status eines „zugelassenen Wirtschaftsbeteiligten" (Authorised Economic Operator – AEO) im Sinne des Unionszollkodex (UZK) und der Erteilung eines AEO-Zertifikates.

Wie die Nachweisführung zu erfolgen hat, ist in den verschiedenen europäischen Rechtsakten nicht geregelt. Jedoch verlangt die Bundeszollverwaltung zwingend einen regelmäßigen Abgleich des in sicherheitsrelevanten Bereichen eingesetzten Personals gegen die Anti-Terror-Listen. Auch hier geschieht der Listenabgleich zu Zwecken des Beschäftigungsverhältnisses, da es sich um Unternehmen handelt, die für den Bereich des grenzüberschreitenden Warenverkehrs bestimmte Erleichterungen bei der Abwicklung ihrer Tätigkeit, wie sie mit den AEO-Zertifikaten verbunden sind, in Anspruch nehmen wollen und die Erteilung dieser Zertifikate von Sicherheitsvorkehrungen in Form einer Überprüfung das Personals abhängig gemacht wird. Die Erforderlichkeit des Listenabgleichs kann bejaht werden, weil bei stark vom internationalen Handel abhängigen Verantwortlichen der Verzicht auf eine AEO-Zertifizierung zu erheblichen Nachteilen im Wettbewerb führen kann, die im Einzelfall existenzgefährdende Ausmaße annehmen können. Ohne Zertifizierung ist die Zollabwicklung mit einem deutlich höheren Aufwand verbunden, sodass Unternehmen mit hohem Zollumschlag ohne Zertifizierung kaum am Markt bestehen können.

Unter Zurückstellung von Bedenken ob des rasterfahndungsartigen Charakters der Anti-Terror-Mitarbeiterscreenings kann dieses auch im zweiten Fall auf § 26 Abs. 1 S. 1 BDSG gestützt werden, obgleich es wünschenswert wäre, dass der Gesetzgeber eine diesbezügliche explizite Regelung schafft.

Da es sich bei den in Rede stehenden Listenabgleichen um Eingriffe hoher Intensität handelt, ist der Grundsatz der Verhältnismäßigkeit dadurch erhöht Rechnung zu tragen, dass Screening-Maßnahmen auf das absolut erforderliche Minimum beschränkt werden. Dies kann durch die Wahl eines angemessenen großen Intervalls bewerkstelligt werden. Auch hier sind wieder die unternehmensspezifischen Besonderheiten zu beachten. Sofern im Einzelfall kein konkreter Anlass besteht, ist ein jährlicher anlassloser Abgleich nicht zu beanstanden.

In sicherheitsrelevanten Bereichen, beispielsweise der Rüstungs- oder Atomindustrie, sowie bei erhöhter Risikolage kann allerdings eine engmaschigere Prüffrequenz angezeigt sein.

Ein Abgleich aller der in der Terrorliste enthaltenen Daten mit den im Unternehmen vorliegenden Beschäftigtendaten ist aber nicht angezeigt. Abgeglichen werden soll-ten ausschließlich diejenigen Daten, die zur eindeutigen Identifizierung eines Beschäftigten unbedingt notwendig sind. Dies sind in aller Regel der Vor- und der Nachname. Lediglich im Falle eines konkreten Verdachts oder bei Zweifeln an der Identität einer Person, beispielsweise bei übersetzungsbedingten abweichenden Namensschreibweisen, kann ein Abgleich weiterer Identifikationsmerkmale angezeigt sein. Aufgrund der erhöhten Eingriffsintensität und um dem Grundsatz der Datenminimierung Rechnung zu tragen, ist es sinnvoll, die Listenabgleiche unternehmensintern vorzunehmen, damit ein weiterer Übermittlungsvorgang an einen das Screening durchführenden Dienstleister vermieden wird. Wird ein solcher eingeschaltet, handelt es sich um eine Auftragsverarbeitung, welche sich an den in der DS-GVO niedergelegten Anforderungen messen lassen muss.

VI. Das Recht auf Erhalt einer Kopie im Arbeitsverhältnis

Wiederholte Beschwerden zu Auskunftsansprüchen gegenüber ehemaligen Arbeitgebern weisen nach Ansicht des LfDI darauf hin, dass insb. das „Recht auf Erhalt einer Kopie"

nach Art. 15 Abs. 3 DS-GVO nicht selten instrumentalisiert wird, um einem ehemaligen Arbeitgeber möglichst viele Unannehmlichkeiten zu bereiten bzw. um durch ein eingeleitetes Bußgeldverfahren die eigene Verhandlungsposition in Bezug auf die Höhe ihrer Abfindung zu verbessern. Auch in Anbetracht der von der Rechtsprechung unterschiedlich gezogegen Reichweite des Anspruchs auf Kopien (LAG Baden-Württemberg , Urt. v. 20.12.2018 – AZ: 17 Sa 11/18 bzw. LG Köln, Urt. v. 18.3.2019 – 26 O 25/18) vertritt der LfDI derzeit folgende Position: „Sofern spezialgesetzliche Regelungen, wie dies im Bereich des Beschäftigtendatenschutz in Bezug auf die Personalakte der Fall ist, das Recht auf Akteneinsichtnahme regeln, handelt es sich hierbei um das am weitesten gehende Recht. Im Rahmen einer Akteneinsichtnahme kann der (ehemalige) Beschäftigte auch Kopien verlangen. Der Arbeitgeber hat dem nachzukommen, sofern dies nicht mit einem unverhältnismäßigen Aufwand (z.B. aufgrund des Umfangs der Personalakte) verbunden ist.“ Andererseits sei der Arbeitgeber aber nicht verpflichtet, sämtliche personenbezogene Daten des Beschäftigten (z.B. aus vorangegangenem E-Mail-Verkehr oder aus sonstigen Sachakten) bei der Geltendmachung des Rechts auf Erhalt einer Kopie zusammenzutragen.

VII. Bußgelder gegen öffentlich Bedienstete

Polizeibeamte, die zu privaten Zwecken Personenabfragen in polizeilichen Informationssystemen vorgenommen haben, können nach einer neuen Regelung im Landesdatenschutzgesetz mit einem Bußgeld belegt werden. § 24 LDSG eröffnet diese Möglichkeit gegenüber einem Beschäftigten im Falle eines sog. Exzesses. Dies ist insbesondere bei ausschließlich privat motivierten Datenabfragen und -nutzungen der Fall. Sofern dem LfDI solche Fälle bekannt wurden, wurden Bußgeldverfahren gegen die Beamten eingeleitet.

Praxisfälle zum Datenschutzrecht IX: Veröffentlichung von Beschäftigtendaten im Unternehmen und außerhalb

Miriam Claus, LL.M./RAin Yvette Reif, LL.M.*

I. Sachverhalt

Unternehmen U möchte für seine Beschäftigten und Kunden/Kundinnen kommunikativer und transparenter werden. Dazu plant die Geschäftsführung, im Intranet des Unternehmens unter der Rubrik „Personalia“ über die Einstellung von neuen Beschäftigten unter Angabe von Namen, Funktion, dienstlichen Kontaktdaten bzw. das Ausscheiden von Beschäftigten zu informieren. Ferner soll unter der Rubrik zu Dienstjubiläen und runden Geburtstagen gratuliert werden.

Im Hinblick auf die Außenkommunikation ist vorgesehen, dass Geschäftsführung, Abteilungsleiter/innen, Außendienstmitarbeiter/innen sowie Sekretariatsmitarbeiter/innen auf der öffentlichen Website des Unternehmens jeweils mit Namen, Zuständigkeit, dienstlichen Kontaktdaten und Foto freundlich dargestellt werden sollen.

Ist das Vorhaben datenschutzrechtlich zulässig?

II. Musterfalllösung

1. Unternehmensinterne Veröffentlichung von „Personalia“ im Intranet

Es stellt sich die Frage, ob die betriebsinterne Veröffentlichung im Intranet zur Durchführung des Beschäftigungsverhältnisses gem. § 26 Abs. 1 S. 1 BDSG erforderlich ist.

Die Erforderlichkeit einer Veröffentlichung zur Durchführung des Beschäftigungsverhältnisses setzt voraus, dass diese im Zusammenhang mit der Wahrnehmung von arbeitsvertraglichen Rechten oder Pflichten steht. Insoweit ist der Gegenstand der veröffentlichten Information von entscheidender Bedeutung.

Ferner wird bei der Prüfung der Erforderlichkeit, die nicht voraussetzt, dass das Verfahren der einzig mögliche und damit unvermeidbare Weg zur Erreichung der verfolgten Zwecke ist, zu bestimmen sein, ob die Veröffentlichung im Hinblick auf ggf. entgegenstehende Interessen der Beschäftigten verhältnismäßig ist.

Typischerweise wird es für die Arbeitsabläufe im Unternehmen nicht erforderlich sein, dass alle Beschäftigten über sämtliche Personalveränderungen informiert werden. Regelmäßig genügt es, Personalwechsel nur insofern allgemein bekanntzugeben, wie diese für die Organisation des Betriebs maßgebende Stellen betreffen, z.B. die Einstellung eines neuen Personalleiters. Im Übrigen reicht es grundsätzlich, ausschließlich diejenigen Beschäftigten über Personalveränderungen zu informieren, für welche die konkrete Veränderung praktisch relevant ist, weil sie mit der betreffenden Person zusammenarbeiten. Etwas anderes mag ausnahmsweise in kleinen Unternehmen bzw. Organisationen gelten, wo sich ohnehin alle Mitarbeiter persönlich kennen.

Zwischenergebnis: Soweit bezogen auf die konkrete Position die allgemeine Kommunikation der Personalveränderung für die unternehmerischen Abläufe geboten ist, ist der Weg der Veröffentlichung im Intranet unter Beachtung des

* Miriam Claus, LL.M. ist Referentin bei der Gesellschaft für Datenschutz und Datensicherheit e.V. (GDD). RAin Yvette Reif, LL.M. ist stellvertretende Geschäftsführerin der GDD und Mitautorin des Werks Gola/Reif, Praxisfälle Datenschutzrecht, 2. Aufl. 2016.

Prinzips der Verhältnismäßigkeit als erforderlich anzusehen und daher gem. § 26 Abs. 1 S. 1 BDSG rechtmäßig.

Entsprechendes gilt, sofern die dienstlichen Kontaktdaten neueingestellter Beschäftigter sowie deren Funktion unternehmensintern allgemein bekanntgegeben werden sollen. Dies ist datenschutzrechtlich nur zulässig, soweit es aufgrund der konkreten Funktion der betroffenen Beschäftigten im Unternehmen erforderlich ist. Sollen Kontakt- und Zuständigkeitsinformationen von Beschäftigten konzernweit geteilt werden, z.B. im Rahmen von konzernweiten Verzeichnissen, ist vor Aufnahme zu prüfen, inwiefern die im Rahmen der konkreten Tätigkeit erwarteten konzernweiten Kontakte eine Publizität in diesem Ausmaß erforderlich machen. Entscheidend ist insoweit eine Einzelfallbetrachtung bzw. eine typisierende Betrachtung auf Basis von gleichartigen Gruppen von Beschäftigten. Ggf. kann ein Verzeichnis auch mittels Zugriffsberechtigungen in unterschiedliche Funktionsbereiche unterteilt werden, um mit vertretbarem Aufwand eine Beschränkung der Reichweite bzw. Publizität zu erreichen.

Fraglich ist, ob die unternehmensöffentliche Würdigung von Betriebsjubiläen unter dem Zweck der Durchführung des Beschäftigungsverhältnisses als erforderlich angesehen werden kann. Die Betriebstreue eines Mitarbeiters bringt dessen enge Verbundenheit mit dem Unternehmen zum Ausdruck, welche durch die interne Veröffentlichung danksagend gewürdigt werden soll. Zugleich soll mit entsprechenden Veröffentlichungen zur Pflege des Betriebsklimas beigetragen werden. Die Veröffentlichung von Betriebsjubiläen steht zwar im Zusammenhang mit dem Beschäftigungsverhältnis, allerdings kann dieses zweifelsohne auch ohne Veröffentlichung von Jubiläen durchgeführt werden. Die interne Veröffentlichung ist damit nicht über § 26 Abs. 1 S. 1 BDSG gerechtfertigt.

Fraglich ist, ob neben § 26 Abs. 1 S. 1 BDSG auch Art. 6 Abs. 1 S. 1 lit. f DS-GVO, also die Interessenabwägung als Rechtsgrundlage in Betracht kommt. Zwar ist, obwohl der Wortlaut dies nicht deutlich macht, § 26 BDSG keine abschließende Regelung für die Verarbeitung von Beschäftigtendaten.[1] Grundsätzlich kann daher auch eine Verarbeitung von Beschäftigtendaten über Art. 6 Abs. 1 S. 1 lit. f DS-GVO legitimiert sein. Bei gleichzeitigem Bestehen eines Vertragsverhältnisses muss Art. 6 Abs. 1 S. 1 lit. f DS-GVO allerdings einschränkend ausgelegt werden, da ansonsten die sich aus Art. 6 Abs. 1 S. 1 lit. b DS-GVO bzw. § 26 Abs. 1 S. 1 BDSG ergebende Beschränkung auf vertraglich erforderliche Datenverarbeitungen ausgehöhlt würde. Die nicht auf vertragliche Erforderlichkeit abstellende Rechtsgrundlage in Art. 6 Abs. 1 S. 1 lit. f DS-GVO findet nur Anwendung, wenn Zwecke verfolgt werden, die nicht unmittelbar auf das Beschäftigungsverhältnis, d.h. die Rechtsbeziehung Arbeitgeber-Beschäftigter bezogen sind.[2] Wie bereits ausgeführt, steht die Veröffentlichung von Betriebsjubiläen zwar im Zusammenhang mit dem Beschäftigungsverhältnis. Sie betrifft aber nicht die vertragliche Beziehung zwischen Arbeitgeber und Beschäftigtem, da kein Zusammenhang zu Rechten und Pflichten aus dem Beschäftigungsverhältnis besteht. Ein Rückgriff auf Art. 6 Abs. 1 S. 1 lit. f DS-GVO ist damit vorliegend möglich.

Nach Art. 6 Abs. 1 lit. f DS-GVO ist eine Datenverarbeitung gestattet, soweit diese zur Wahrung der berechtigten Interessen des Verantwortlichen oder eines Dritten erforderlich ist und nicht die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person, die den Schutz personenbezogener Daten erfordern, überwiegen. Der verantwortliche Arbeitgeber verfolgt vorliegend mit der Pflege des Betriebsklimas ein berechtigtes Interesse. Fraglich ist, ob schutzwürdige Interessen des Beschäftigten überwiegen.

Bezüglich der Bekanntgabe der Jubiläen erscheint es – unter Berücksichtigung der Umstände des jeweiligen Einzelfalls – prinzipiell vertretbar, dies jedenfalls dann nicht anzunehmen, wenn die Beschäftigten zuvor entsprechend informiert wurden und ihnen im Vorfeld der konkreten Veröffentlichung eine Widerspruchsmöglichkeit gegen diese gem. Art. 21 Abs. 1 DS-GVO eingeräumt wurde, von der kein Gebrauch gemacht wurde. Hat der Beschäftigte einer Verarbeitung auf Grundlage von Art. 6 Abs. 1 S. 1 lit. f DS-GVO widersprochen, ist der Verantwortliche gem. Art. 21 Abs. 1 S. 2 DS-GVO nicht mehr berechtigt, die personenbezogenen Daten zu verarbeiten, solange er keine zwingend schutzwürdigen Gründe für die Verarbeitung nachweisen kann, welche die Interessen des Beschäftigten überwiegen. Von einem überwiegenden Interesse des Arbeitgebers kann bei der Veröffentlichung von Betriebsjubiläen nicht ausgegangen werden. Dies würde auch dem ursprünglichen Zweck der Stärkung des Betriebsklimas zuwiderlaufen.

Freilich muss der Arbeitgeber nicht auf die gesetzliche Verarbeitungserlaubnis aus Art. 6 Abs. 1 S. 1 lit. f DS-GVO zurückgreifen, sondern kann sich stattdessen auch dafür entscheiden, die Veröffentlichung im Intranet nur in Absprache mit den betroffenen Beschäftigten und auf Basis einer Einwilligung entsprechend § 26 Abs. 2 BDSG durchzuführen. Eine Einwilligung sollte jedenfalls dann eingeholt werden, wenn zusätzlich Informationen zum persönlichen Werdegang des Mitarbeiters veröffentlicht werden sollen.

Auch im Hinblick auf die Veröffentlichung von Geburtstagen ist ein Rückgriff auf Art. 6 Abs. 1 S. 1 lit. f DS-GVO prinzipiell möglich. Bei der Veröffentlichung von Geburtstagen ist hingegen fraglich, ob eine Widerspruchslösung als ausreichend zu bewerten ist. Dagegen spricht, dass anders als bei Betriebsjubiläen mit dem Geburtstag die persönliche Sphäre des Mitarbeiters betroffen ist. Auch empfinden viele Personen ihren Geburtstag bzw. ihr Alter als sensible Information. Die Entscheidung über die Veröffentlichung solcher Daten muss beim Beschäftigten verbleiben, demnach kann insoweit nur mit einer Einwilligung gem. § 26 Abs. 2 BDSG eine rechtmäßige Verarbeitung erfolgen.

Zwischenergebnis: Die betriebsinterne Veröffentlichung von Betriebsjubiläen ist gem. Art. 6 Abs. 1 S. 1 lit. f DS-GVO statthaft, sofern den Beschäftigten die Möglichkeit des Widerspruchs eingeräumt wird. Eine Veröffentlichung von Geburtstagen ist ohne Einwilligung nicht zulässig.

Ergebnis: Das Vorhaben von U ist unter den beschriebenen, je nach Datum unterschiedlichen Zulässigkeitsvoraussetzungen umsetzbar.

1 Gola, Handbuch Beschäftigtendatenschutz, 8. Aufl. (2019), Rn. 748.

2 Gola, a.a.O., Rn. 755.

2. Veröffentlichung von Beschäftigtendaten auf der Unternehmenshomepage

a) Allgemeines

Im Hinblick auf die Veröffentlichung von Beschäftigtendaten im Internet gilt der gleiche Maßstab wie hinsichtlich der unter Ziff. 1 geprüften Veröffentlichung im Intranet. Entscheidend ist, ob die Veröffentlichung – hier im Internet, nicht im Intranet – zur Durchführung des Beschäftigungsverhältnisses erforderlich ist (§ 26 Abs. 1 S. 1 BDSG). Maßstab für die Zulässigkeit der Veröffentlichung von Beschäftigtendaten im Internet ist, inwiefern die vertraglich vereinbarte Tätigkeit auch Außenkontakte mit sich bringt und der Beschäftigte als direkter Ansprechpartner fungieren soll.[3] Im Rahmen der bei der Prüfung der Erforderlichkeit notwendigen Verhältnismäßigkeitsprüfung ist im Hinblick auf Internetveröffentlichungen zu beachten, dass eine Veröffentlichung von personenbezogenen Daten im Internet von jedermann global abrufbar ist und die gefunden Informationen zu einer Person ggf. mit weiteren im Netz vorhandenen Daten zu Persönlichkeitsprofilen zusammengeführt werden können.[4] Internetveröffentlichungen haben also eine deutlich größere Eingriffsintensität als Veröffentlichungen im Intranet. Für die Durchführung des Beschäftigungsverhältnisses gem. § 26 Abs. 1 BDSG erforderlich kann etwa die Internetveröffentlichung von Namen, Funktion sowie dienstlichen Kontaktdaten bspw. von Geschäftsführern/Geschäftsführerinnen, Außendienstmitarbeitern/-mitarbeiterinnen, Kundenbetreuern/-betreuerinnen oder des/der Pressesprechers/-sprecherin sein.[5] In die Beurteilung der Erforderlichkeit sollte allerdings einbezogen werden, ob ggf. die Verwendung einer Funktions- statt einer namensbezogenen Mailadresse möglich ist. Der Arbeitgeber hat zudem dafür zu sorgen, seinen Internetauftritt so zu konfigurieren, dass Mitarbeiter nicht ohne weiteres von Suchmaschinen wie Google gefunden werden können.[6]

b) Besonderheiten im Hinblick auf die Veröffentlichung von Fotos

Im Hinblick auf die Veröffentlichung von Fotos ist zunächst die Frage nach den einschlägigen Regelungen zu klären. Zu erörtern ist, ob für die Veröffentlichung der Mitarbeiterfotos das Kunsturhebergesetz (KunstUrhG) einschlägig ist oder aber die DS-GVO bzw. das BDSG.

Eindeutig ist, dass sich etwa das Anfertigen und Speichern von Fotos ausschließlich nach der DS-GVO richtet, weil diese Sachverhalte vom KunstUrhG, welches sich nur mit der Verbreitung bzw. öffentlichen Zurschaustellung von Bildnissen befasst, nicht erfasst sind.

Im Übrigen hat das BAG[7] zwar im Jahr 2014 entschieden, dass das KunstUrhG für die Frage der Einwilligung in die Verwertung und den Widerruf dieser Einwilligung als spezielleres und bereichsspezifisches Gesetz gegenüber den Regelungen des BDSG a.F. Vorrang habe. Das Gericht bezog sich in seiner Entscheidung insofern auf die Subsidiaritätsklausel in § 1 Abs. 3 Satz 1 BDSG a.F., wonach „andere Rechtsvorschriften des Bundes … soweit sie auf personenbezogene Daten einschließlich deren Veröffentlichung anzuwenden sind“, den Vorschriften des BDSG „vorgehen“.

Eine ähnliche Regelung ist auch im aktuell gültigen BDSG enthalten (§ 1 Abs. 2 S. 1 BDSG). Dieses regelt allerdings auch, dass die Vorschriften dieses Gesetzes keine Anwendung finden, soweit das Recht der Europäischen Union, im Besonderen die DS-GVO in der jeweils geltenden Fassung, unmittelbar gilt. Dieser Anwendungsvorrang der unmittelbar geltenden DS-GVO macht es fraglich, ob die BAG Entscheidung aus dem Jahr 2014 heute noch einmal mit gleichem Inhalt ergehen könnte. Auch die durch Art. 85 bzw. Art. 88 DS-GVO gegenüber den Mitgliedstaaten eingeräumten Gestaltungsspielräume ändern an diesen Zweifeln nichts. Mit der Verwendung von Mitarbeiterfotos im Internet werden regelmäßig keine in Art. 85 DS-GVO genannten Zwecke, etwa journalistische[8] oder künstlerische Zwecke, verfolgt. Da die § § 22, 23 KunstUrhG sich nicht spezifisch auf den Beschäftigungskontext beziehen, wird auch Art. 88 DS-GVO als Grundlage für eine weitere Anwendung des KunstUrhG zumindest im Beschäftigungsverhältnis ausscheiden.[9]

Die Beurteilung der Veröffentlichung der Mitarbeiterfotos richtet sich damit vorliegend ausschließlich nach der DS-GVO bzw. dem BDSG.[10]

Für eine direkte Kontaktaufnahme mit der entsprechenden Person ist die Veröffentlichung von Fotos allerdings nicht erforderlich, so dass § 26 Abs. 1 S. 1 BDSG als Rechtsgrundlage ausscheidet. Ein Rückgriff auf Art. 6 Abs. 1 S. 1 lit. f DS-GVO kommt in diesem Fall nicht in Betracht. Mit der Erreichbarkeit für die Ansprache durch Kunden bzw. Interessenten wird vorliegend ein Zweck verfolgt, der unmittelbar auf das Beschäftigungsverhältnis bezogen ist. Würde man hier einen Rückgriff auf die Interessenabwägung gestatten, käme es zu einer Aushöhlung des Erforderlichkeitsprinzips im Rahmen von Art. 6 Abs. 1 S. 1 lit. b DS-GVO.[11] Im Ergebnis kommt die Veröffentlichung der Fotos damit nur auf Grundlage einer Einwilligung in Betracht, wobei die besonderen Anforderungen an die Einwilligung von Beschäftigten nach § 26 Abs. 2 BDSG zu beachten sind.

Nach § 26 Abs. 2 BDSG bestehen besondere Formanforderungen an die Einwilligung von Beschäftigten. Während nach der DS-GVO Einwilligungen formfrei erteilt werden können, muss nach § 26 Abs. 2 BDSG bei der Einwilligung von Beschäftigten grundsätzlich die Schriftform oder elektronische Form gewahrt werden, es sei denn, wegen besonderer

3 LfDI Baden-Württemberg, Ratgeber Beschäftigtendatenschutz, 4. Aufl. (2020), S. 42 (abrufbar unter: https://t1p.de/vfy7 (zuletzt abgerufen am 15.02.2021)).

4 LfDI Baden-Württemberg, ebenda.

5 Koreng/Lachenmann/Bergt, Formularhandbuch Datenschutzrecht, 2. Aufl. 2018, H. I. 1., Rn. 1.

6 LfDI Baden-Württemberg, ebenda.

7 BAG, Urt. v. 11.12.2014 – 8 AZR 1010/13.

8 Entsprechend der Rechtsprechung zum Medienprivileg nach § 41 BDSG a.F. wird man eine journalistische Tätigkeit nur im Fall „organisatorisch in sich geschlossener, gegenüber den sonstigen (betrieblichen) Stellen abgeschotteter, in der redaktionellen Tätigkeit autonomer Organisationseinheiten“ annehmen können, vgl. BVerwG, Beschluss vom 29.10.2015 – 1 B 32.15.

9 Assmus/Winzer, ZD 2018, 508 (512) m.w.N.

10 So auch Assmus/Winzer, ZD 2018, 508 (513); Benedikt/Kranig, ZD 2019, 4 (6); LfDI Baden-Württemberg, Ratgeber Arbeitnehmerdatenschutz, 4. Auflage (2020), S. 44.

11 Vgl. dazu oben unter II.1.

Umstände ist ausnahmsweise eine andere Form angemessen. Der Arbeitgeber muss die beschäftigte Person zudem in Textform über den Zweck der Datenverarbeitung sowie ihr Widerrufsrecht nach Art. 7 Abs. 3 DS-GVO aufklären.

Außerdem verlangt § 26 Abs. 2 BDSG, dass bei Einwilligungen im Beschäftigungsverhältnis wegen des bestehenden Abhängigkeitsverhältnisses zwischen Beschäftigtem und Arbeitgeber jeweils eine besondere Prüfung der Freiwilligkeit der Erklärung erfolgt. Die gesetzlichen Regelbeispiele in § 26 Abs. 2 S. 2 BDSG, in denen von einer Freiwilligkeit der Erklärung ausgegangen werden kann, sind vorliegend nicht einschlägig. Der Arbeitgeber muss also deutlich machen, dass die Beschäftigten mit Außenkontakt frei entscheiden können, ob auch ihr Bild veröffentlicht werden soll oder nicht. Es darf kein Druck ausgeübt werden, etwa in Form der Aussage, alle anderen hätten auch ihre Einwilligung erteilt. Widerruft der Beschäftigte eine zunächst abgegebene Einwilligung in die Veröffentlichung, ist sein Bild wieder zu löschen.

Wie bereits im Abschnitt a) erwähnt, sind Unternehmen zudem gehalten, durch entsprechende technische und organisatorische Maßnahmen eine Auffindbarkeit der Mitarbeiter in Suchmaschinen wie Google zu unterbinden. Mitarbeiterdaten und Fotos auf Unternehmenswebseiten sollen nicht die Bildung von Persönlichkeitsprofilen unterstützen.

c) Ergebnis

Das Vorhaben von U, Kontaktdaten sowie Mitarbeiterfotos auf der Unternehmenswebseite zur veröffentlichen, ist datenschutzrechtlich umsetzbar. Bezüglich der Kontaktdatenveröffentlichung ist insbesondere darauf zu achten, dass die Veröffentlichung nur für Beschäftigte erfolgt, die nach Art ihrer Tätigkeit als direkte, namensbezogene Ansprechpartner nach außen fungieren. Fotos dürfen nur mit Einwilligung der betroffenen Beschäftigten ins Internet gestellt werden, wobei bei der Einholung kein Druck ausgeübt werden darf.

3. Praxishinweise

Wenn Fotos nicht – wie bei Einzelaufnahmen – schnell zu entfernen sind oder für festgelegte Zwecke über einen längeren Zeitraum zur Verfügung stehen sollen, sollte mit den abgebildeten Beschäftigten ein separater Vertrag über die Anfertigung und Verwendung der Aufnahmen geschlossen werden. Beispielhaft sind hier Gruppenfotos zur Unternehmenspräsentation. Hier müsste bei erfolgtem Widerruf der Einwilligung die betroffene Person in der Form unkenntlich gemacht werden, dass keine Identifizierung mehr möglich ist. Dies ist für den Verantwortlichen aber regelmäßig keine Option. Ein Gruppenfoto mit verpixelten Personen ist zu Repräsentationszwecken nicht brauchbar.

Betriebsrätestärkungsgesetz und Datenschutz – voll eigenverantwortlich „ohne“ Verantwortlichkeit

Mit obiger Überschrift haben Dr. Stefan Brink, Landesbeauftragter für den Datenschutz und die Informationsfreiheit Baden-Württemberg und Daniel Joos, Referent für Beschäftigtendatenschutz zum am 21.12.2020 vorgelegten Referentenentwurf des Gesetzes zur Förderung der Betriebsratswahlen und zur Stärkung der Betriebsräte (Betriebsrätestärkungsgesetz) (Referentenentwurf des Gesetzes zur Förderung der Betriebsratswahlen und zur Stärkung der Betriebsräte (Betriebsrätestärkungsgesetz) (abrufbar unter: https://www.bmas.de/SharedDocs/Downloads/DE/PDF-Gesetze/Referentenentwuerfe/ref-entwurf-zur-foerderung-derbetriebsratswahlen-und-zur-staerkung-der-betriebsraete.pdf;jsessionid=883B3965048 F103A5FFB6E1D3F43C36D.delivery2-master?__blob=publicationFile&v=2, zuletzt abgerufen am 26.01.2021) und den in ihm enthaltemen Regelungen hinsichtlich des Datenschutzes und der Einhaltung datenschutzrechtlicher Vorschriften durch den Betriebsrat als betrieblicher Funktionsträger die hier zusammengefasste Stellungnahme abgegeben (vgl. https://www.juris.de/jportal/portal/page/homerl.psml?nid=jpr-NLARA).

Nach dem RefE soll die datenschutzrechtliche Verantwortlichkeit nach der DS-GVO für die Verarbeitung der personenbezogenen Beschäftigtendaten durch den Betriebsrat formal dem Arbeitgeber zugewiesen sein. Gleichzeitig wird der Betriebsrat aber auch verpflichtet (vgl. § 79a), „eigenverantwortlich [für] die Umsetzung technischer und organisatorischer Maßnahmen“ zu sorgen, was eigentlich als grundlegende Verpflichtung der verantwortlichen Stelle i.S.d. Art. 4 Nr. 7 DS-GVO obliegt.

Daneben enthält der RefE in § 79a den Versuch der gesetzgeberischen Klarstellung der bislang in Gesetzgebung und Rechtsprechng unterschiedlich gesehenen datenschutzrechtlichen Verantwortlichkeit des Betriebsrats. Während einzelne Landesarbeitsgerichte nunmehr eine eigene datenschutzrechtliche Verantwortlichkeit des Betriebsrats annehmen (LAG Rostock, Beschl. v. 15.05.2019 – 3 TaBV 10/18 m. Anm. Brink/Joos, jurisPR-ArbR 33/2019 Anm. 1; LAG Halle, Beschl. v. 18.12.2018 – 4 TaBV 19/17), wird diese von weiten Teilen der Rechtsprechung und der Literatur nach wie vor abgelehnt. Dementsprechend hatte die DSK (Konferenz der Datenschutzbeauftragten der Länder und des Bundes) – ohne sich auf eine einvernehmliche Lösung festzulegen – den Bundesgesetzgeber aufgefordert, eine gesetzliche Entscheidung zur Verantwortlichkeit von Betriebsräten zu treffen.

In § 79a des Referentenentwurfs wird nunmehr mit der Argumentation, dass der Betriebsrat keine nach außen rechtlich verselbstständigte Institution“ sei, klargestellt, dass „der Arbeitgeber der für die Verarbeitung Verantwortliche i.S.d. datenschutzrechtlichen Vorschriften“ ist. wobei der Realität Rechnung tragend eigeräumt wird, dass bei Auskunftsersuchen, welche „sich auf die durch den Betriebsrat verarbeiteten Daten bezieht, [der Arbeitgeber] auf

die Unterstützung durch den Betriebsrat angewiesen“ ist, obwohl die Datenverarbeitungen des Betriebsrats dem Einfluss des Arbeitgebers aus gutem Grund mit Blick auf die Vertraulichkeit einzelner Vorgänge und oftmals widerstreitenden Interessen entzogen sein sollten. Auf der anderen Seite sieht der Referentenentwurf vor, dass der Betriebsrat „eigenverantwortlich [für] die Umsetzung technischer und organisatorischer Maßnahmen“ zuständig ist, was aber eine originäre Aufgabe der verantwortlichen Stelle aus datenschutzrechtlicher Sicht ist.

Die Autoren kommen letztendlich zu der Auffassung, dass dieavisierte Regelung des § 79a des Referentenentwurfs aus datenschutzrechtlicher Sicht nicht konsequent sei, da sie dem Betriebsrat eigenverantwortliche Aufgaben zuweist, ohne ihn dogmatisch zum Verantwortlichen zu erklären.

Gehaltszettel im Kindergartenrucksack: – LfDI rügt „unbürokratische“ Datenübermittlung –

Der LfDI Rheinland-Pfalz musste sich gemäß seinem 28. TB (vom 12.01.2021) im Rahmen einer Beschwerde mit den datenschutzrechtlichen Anforderungen an die Zustellung von Entgeltabrechnungen einer Gemeinde auseinandersetzen.

Der Beschwerdeführer war bei einer Ortsgemeinde beschäftigt und hatte seine Dienstherrin aufgrund einer längeren Erkrankung darum gebeten, seine Entgeltabrechnungen bis auf Weiteres übersandt zu bekommen. Statt dem Beschwerdeführer die Entgeltabrechnung auf postalischem Wege zur Verfügung zu stellen, bediente sich die Dienstherrin der Einfachheit halber des Kindergartenrucksacks des Sohnes des Beschwerdeführers, welcher die Kindertagesstätte der Ortsgemeinde besuchte, als Übermittlungsmedium. Dort fand die Lebensgefährtin des Beschwerdeführers die Entgeltabrechnung abends vor.

Diese Art der Übermittlung entsprach nach Auffassung des LfDI nicht den technisch-organisatorischen Anforderungen nach Art. 32 DS-GVO. Der Arbeitgeber bzw. Dienstherr ist nach § 108 Abs. 1 Gewerbeordnung und der Entgeltbescheinigungsverordnung verpflichtet, dem Arbeitnehmer eine Entgeltbescheinigung in Textform zur Verfügung zu stellen. Diese muss dergestalt auf den Weg zu dem oder der Beschäftigten gebracht werden, dass sie in dessen oder deren Machtbereich gelangt und der oder die Beschäftigte sodann unter gewöhnlichen Umständen von der Abrechnung Kenntnis nehmen kann. Die Art und Weise, wie dieser Verpflichtung entsprochen wird, ist ein zum Rechtskreis des Arbeitgebers/Dienstherrn zugehöriges Geschäft. Dementsprechend muss der Arbeitgeber/ Dienstherr bei der Wahl des Übertragungsweges auch die erforderlichen technisch-organisatorischen Datenschutzmaßnahmen treffen, um die Gefahr einer Fehlleitung, eines Verlustes oder einer Kenntnisnahme durch Unbefugte weitestgehend auszuschließen. Dem wurde mit der durch die Ortsgemeinde gewählten Form der Übergabe nicht entsprochen.

Literaturhinweise

Gina Rosa Wollinger/Anna Schulze (Hrsg.), **Handbuch Cybersecurity für die öffentliche Verwaltung**, Verlag C.H. Beck, München 2020, 450 S., 69,– €

Mit der Erstauflage des Handbuches Cybersecurity für die öffentliche Verwaltung wollen deren Herausgeberinnen einen Beitrag dazu liefern, die Bedeutung von Cybersecurity, auch über die Mitarbeiter der IT-Abteilung hinaus, verständlich zu transportieren sowie Handlungsmöglichkeiten für die öffentliche Verwaltung aufzuzeigen. Das Handbuch zeichnet sich dabei insbesondere durch die interdisziplinäre Autorenschaft aus den Bereichen der Kriminoogie, Mathematik, Informatik, Psychologie, Soziologie, Politikwissenschaft, Verwaltungswissenschaft, Wirtschaftswissenschaft, Rechtswissenschaft und Digitalen Forensik aus.

Der erste Teil des Handbuchs ist der Beschreibung des Phänomens der Cyberkriminalität gewidmet. Eine einheitliche Definition des Begriffs „Cyber" existiert demnach nicht. Wie im Titel des Handbuchs selbst, verfolgt die Voranstellung des Präfixes den Zweck, einen Bezug zu informationstechnischen Systemen, Internet und Datenverarbeitung herzustellen und beim Leser entsprechende Assoziationen hervorzurufen. Beschrieben werden verschiedene Formen der Bedrohung durch Cyberkriminalität – z.B. in Form von Schadsoftware-Angriffen, Botnetzen, Ransomware, (Distributed) Denial-of-Service Attacken, Spyware, Social Engineering und Phishing –, Täter- und Opferprofile sowie das Ausmaß der Verbreitung von Cyberkriminalität in Deutschland.

Wie Wollinger und Schulze in der Einführung zu ihrem Handbuch konstatieren, haben sich die Kommunikationsverhältnisse in den letzten Jahrzehnten in einer noch nie da gewesenen Geschwindigkeit elementar gewandelt, und unter den Bedingungen von Corona habe sich das Potenzial des Digitalen nochmals in einer neuen Dimension gezeigt. Vor diesem Hintergrund beleuchtet der zweite Teil des Handbuchs die Bedeutung der Digitalisierung für die kommunale Verwaltung, wobei auf bisherige Ansätze zur Digitalisierung im Bereich der Bin-nenverwaltung, aktuelle Entwicklungen im Kontext der Digitalisierung der Kommunalverwaltung sowie Anforderungen an die kommunale Verwaltung im Digitalisierungskontext eingegangen wird. Ein eigenes Kapitel im zweiten Teil des Handbuchs ist der Organisation und Struktur der Digitalisierung der Kommunen gewidmet.

Unter der Überschrift „Informationssicherheit für Kommunen" befasst sich der dritte Teil mit den Grundzügen des Informationssicherheits-/Datenschutzrechts für Kommunen, BSI-Grundschutz und ISO/IEC 27001, technischen Sicherheitsmaßnahmen in Form von Kryptografie und elektronischen Vertrauensdiensten, Mitarbeitersensibilisierung in der Kommunalverwaltung und der Einführung eines IT-Sicherheitsmanagements in der kommunalen Praxis. Praktisch dürfte dabei u.a. dem Punkt „Mitarbeitersensibilisierung" besondere Bedeutung zukommen, denn die beste technische Absicherung der IT-Infrastruktur nützt nichts, wenn kommunale Mitarbeiter im Rahmen von Social Engineering relevante Informationen preisgeben oder arglos auf Anhänge von Phishing Mails klicken. Die Mitarbeiterakzeptanz ist – neben der Nutzerfreundlichkeit – zudem ein zentraler Schlüssel bei der Einführung technischer Sicherheitsverfahren, wie z.B. der Mailverschlüsselung.

Einen wesentlichen Beitrag zur Mitarbeitersensibilisierung können der/die Datenschutzbeauftragte und, sofern vorhanden, der/die IT-Sicherheitsbeauftragte leisten. Eine wichtige Rolle spielen nach Ivona Matas, Autorin des relevanten Kapitels, zudem die gelebte Fehler- und Behördenkultur sowie das Verhalten der Führungskräfte. Bei der Konzeption von Sensibilisierungsmaßnahmen sollten nach Matas u.a. unterschiedliche Lernweisen und psychologische Mechanismen berücksichtigt werden. Ziel sei nicht die (kurzfristige) Information, sondern vielmehr eine im Arbeitsalltag dauerhaft umgesetzte Wachsamkeit für eigene Verhaltensweisen.

Mit Innovationen zur Begegnung von Cyberangriffen in Form von Cyber-Versicherungen und der Block Chain Technologie beschäftigt sich der letzte Teil des Handbuchs.

Das Handbuch bietet damit einen gelungenen Überblick über verschiedene wissenschaftliche Aspekte des Themas Cybersecurity, der zwar nach dem Titel des Handbuchs auf die öffentliche Verwaltung zugeschnitten, aber nicht nur für diese von Relevanz ist. Viele Kapitel enthalten Informationen und geben Impulse, die für Verantwortungsträger in der Privatwirtschaft in gleicher Weise aktuell sind.

(RAin Yvette Reif, LL.M., Bonn)

Louisa Specht-Riemenschneider/Benedikt Buchner/Christian Heinze/Oliver Thomsen (Hrsg.), **Festschrift für Jürgen Taeger: IT-Recht in Wissenschaft und Praxis**, Fachmedien Recht und Wirtschaft, dfv Mediengruppe, Frankfurt/M. 2020, 771 S., 249,– €

Anlässlich seines 65. Geburtstags würdigen zahlreiche, namhafte Freunde und Weggefährten die Verdienste von Prof. Dr. Jürgen Taeger als Wissenschaftler und Hochschullehrer mit einer von Specht-Riemenschneider, Buchner, Heinze und Thomsen herausgegebenen Festschrift, wobei der Begriff „Festschrift" die 771 Seiten ausmachende Großkommentierung aktueller Fragen des Daten- und Informationsrechts nur unzureichend erfasst.

Die Beiträge der über 40 Autoren betreffen Themen aus den Tätigkeitsschwerpunkten von Jürgen Taeger, wie dem Zivil-, dem Wirtschafts- und vor allem dem Informationsrecht. Enthalten sind Beiträge zu den Bereichen des Bürgerlichen Rechts, des Datenschutzrechts, des Informations- und Medienrechts, des Rechts des geistigen Eigentums und der Rechtsdurchsetzung. Dabei geht es zum einen um Grundsatzfragen, wie sie sich z.B. beim Einsatz künstlicher Intelligenz, im Verhältnis von Arbeits- und Datenschutz stellen. Nachgegangen wird aber auch der sich unter verschiedenen Aspekten stellenden Frage des Umfangs datenschutzrechtlicher Verantwortlichkeit und Haftung oder der Wirksamkeit von Einwilligungen oder der Rolle des Arbeitgebers als TK-Dienstleister. Bei den Beiträgen geht es sowohl um allgemeine Anforderungen an das – zukünftige – Datenschutzrecht als auch um praxisbezogene Anwendungsfragen. Wenn auch nicht jede der 43 Abhandlung für den Nutzer des Buches von Interesse sein mag, wird die breite Themenstellung dem Nutzer vielfach zu benötigten Informationen und Neubetrachtungenhelfen.

Das breite Themenspektrum spiegelt aber auch die Vielfalt der Tätigkeiten und Interessen des Geehrten deutlich, dessen nicht nur die Lehre betreffendes Engagement Thomsen in einem die Veröffentlichungabschließenden Beitrag darstellt.

Dazu bleibt anzumerken, dass Jürgen Taeger auch der GDD als Mitglied des wissenschaftlichen Beirats erhalten bleibt und auch wir stolz darauf sind, dass er dieser Zeitschrift als Mitglied des Herausgeberbeirats und regelmäßiger Autor verbunden ist.

(Prof. Peter Gola)

Neuerscheinungen

Aufsätze

Die RDV weist regelmäßig auch auf in anderen Zeitschriften erschienene Beiträge zum Recht der Datenverarbeitung hin, um Recherchen zu relevanten Themen zu erleichtern Einreichungen von Beiträgen zur Aufnahme eines Hinweises werden gerne entgegen genommen.

Brams, Isabell/Wybitul, Tim, **Bußgeld i.H.v. 35,3 Mio. € wegen Mitarbeiterüberwachung – Ein Trend zu hohen Bußgeldern in Deutschland?**, DB 2021, S. 57
Der HmbBfDI hat jüngst gegen ein Unternehmen ein Bußgeld i.H.v. 35,3 Mio. € wegen Datenschutzverstößen verhängt. Nach einem kurzen Überblick über die Entscheidung erläutern die Verfasser die datenschutzrechtlichen Rahmenbedingungen für die Durchführung von Mitarbeiterkontrollen.

Brors, Christiane, **Reform des Arbeitszeitgesetzes – Europäische Vorgaben zur Arbeitszeiterfassung und zum Arbeitnehmerdatenschutz**, NZA 2020, S. 1685
Ausgehend von dem Urteil des EuGH in Sachen CCOO (Urteil vom 14.5.20199 – C-55/18) zeigt die Verfasserin den Umsetzungsbedarf und die Umsetzungsmöglichkeiten im deutschen Recht auf. Sie plädiert für eine Änderung des ArbZG unter Beachtung § 26 Abs. 1 BDSG.

Frank, Justus/Heine, Maurice, **„Corona und die Detektive"? Corona und Keylogger!? Kontrollmöglichkeiten in Zeiten von Home-Office**, BB 2021, S. 248
Erörtert werden verschiedene Kontrollmöglichkeiten von Home-Office-Arbeit vornehmlich datenschutzrechtlich unter § 26 BDSG i.V.m. Art. 88 DS-GVO. Schließlich werden auch die arbeitgeberseitigen Informationspflichten eingehend erörtert.

Franzen, Martin, **Das Verhältnis des Auskunftsanspruchs nach DS-GVO zu personalaktenrechtlichen Einsichtsrechten nach dem BetrVG**, NZA 2020, S. 1593
Aufgezeigt wird das Verhältnis zwischen den Auskunftsrechten nach Art. 15 Abs. 1, Abs. 3 DS-GVO und § 83 Abs. 1 BetrVG. Nach einer Erläuterung der Reichweite der jeweiligen Ansprüche kommt der Autor zu dem Ergebnis, dass Art. 15 DS-GVO durch § 83 Abs. 1 BetrVG verdrängt wird.

Gola, Peter, **Der Auskunftsanspruch nach dem Entgelttransparenzgesetz – ein Statusbericht**, BB 2021, S. 116
Der Verfasser beschäftigt sich in diesem Beitrag mit dem in § 10 Abs. 1 S. 1 EntgTranspG enthaltenem Auskunftsanspruch. Vor allem wird aufgezeigt, welchen rechtlichen Rahmenbedingungen und Grenzen der Auskunftsanspruch unterliegt.

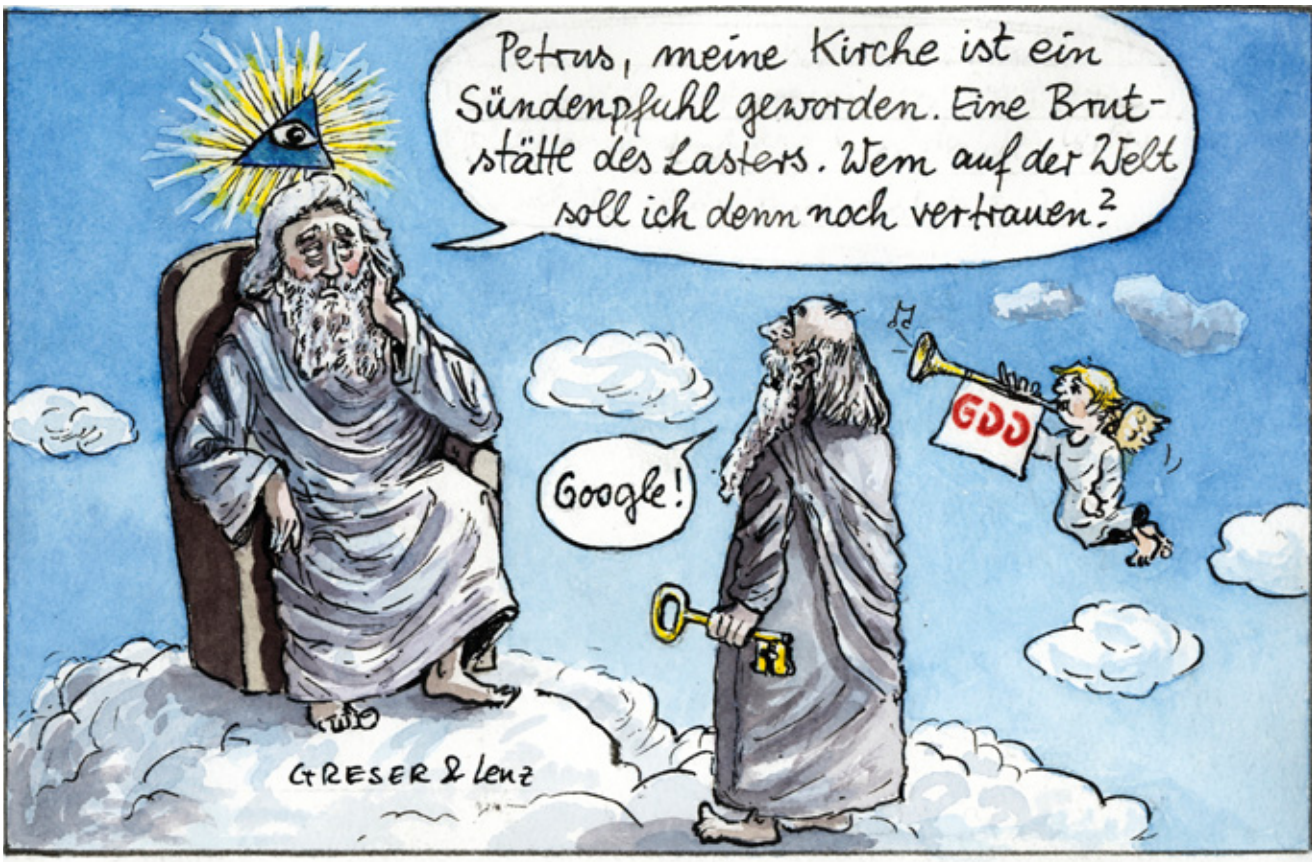
Herberger, Marie, **Die Entfernung einer Abmahnung aus der Personalakte – Eine Betrachtung aus datenschutzrechtlicher Perspektive**, NZA 2020, S. 1665
Aufgezeigt wird der Anspruch auf Entfernung einer Abmahnung aus der Personalakte aus §§ 242, 1004 BGB analog gegenüber einem Anspruch aus Art. 17 DS-GVO. Der Anspruch aus Art. 17 DS-GVO sei für den Arbeitnehmer leichter durchzusetzen.

Köhler, Matthias/Serbina, Tatjana, **Sonderkündigungsschutz des Datenschutzbeauftragten: Sind § 38 Abs. 1 und 2 i.V.m. § 6 Abs. 4 Satz 2 BDSG europarechtskonform?**, DB 2020, S. 2752
Kommentiert wird der diesbezügliche Vorlagebeschluss des BAG vom 30.07.2020 – 2 AZR 225/20 (A).

Siebens,Frank, **Arbeitszeit, Arbeitszeiterfassung, Überstundenvergütung, Beweislast**, AuR 2021, S. 91
Besprochen wird das Urteil des ArbG Emden vom 24.09.2020 – 2 Ca 144/20.

Thüsing, Gregor, **Arbeitszeiterfassung: Keine Aufzeichnungspflichten unmittelbar aus Art. 31 Abs. 2 GrCh!**, DB 2020, S. 1343
Anhand der Entscheidung des EuGH in der Rechtssache CCOO und des Urteils des ArbG Emden beschäftigt sich der Autor insbesondere mit der Frage, inwiefern eine Aufzeichnungspflicht der Arbeitszeit des Arbeitnehmers für den Arbeitgeber besteht und welche Rolle Art. 31 Abs. 2 GrCh dabei spielt.

Tödtmann, Ulrich/Erdmann von, Charlotte, **Keine Pflicht zur Selbstbelastung für den Arbeitnehmer? Auswirkungen des Verbandssanktionsgesetzes und die übersehene Rechtsprechung des BAG**, NZA 2020, S. 1577
Da Arbeitgeber in bestimmten Situationen ein berechtigtes Interesse haben können, über inner- und außerbetriebliche Rechtsverstöße ihrer Arbeitnehmer informiert zu werden, gilt für den Arbeitnehmer gemäß §§ 666, 675 BGB eine Auskunftspflicht. Jedoch kann dies auch zu einer Selbstbelastung des Arbeitnehmers führen. Die Pflicht hierzu wird u.a. im Hinblick auf das Verbandssanktionengesetz skizziert.

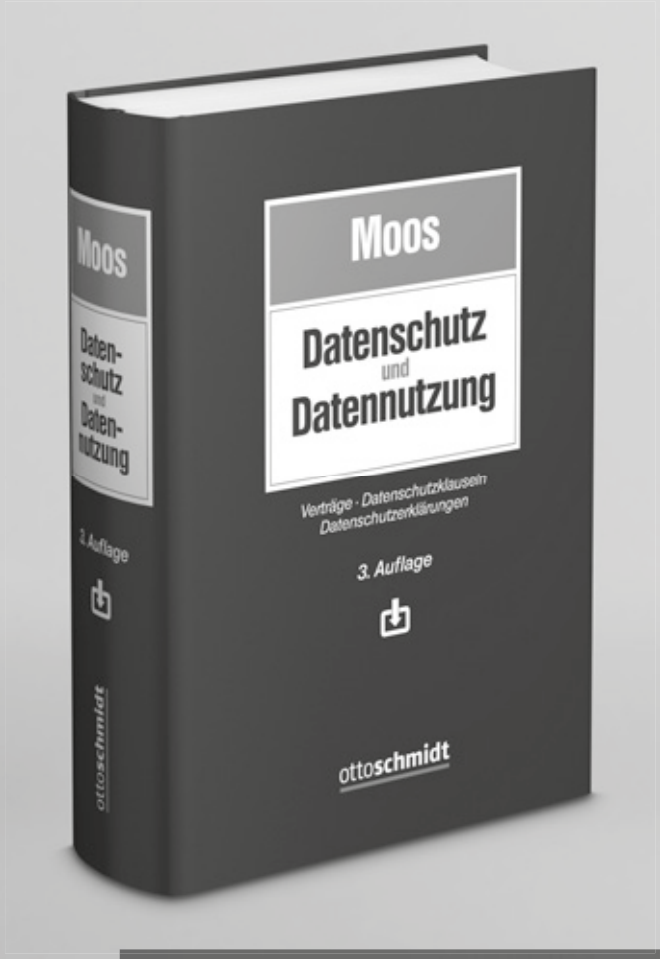


Gottvertrauen 2.0

Meinungsfreiheit á la Google

„Die ‚Titanic-App' kannst du nicht herunterladen. Die machen obszöne Witze, und die haben Dich nicht zu interessieren." Das ist die Meinungsfreiheit im Google Play-Store. Dort herrscht der Tech-Gigant wie ein Kioskbetreiber über sein Sortiment. Worüber man im Play-Store lachen darf, bestimmt das Unternehmen. Weil Google ein Teil der Witze zu obszön war, hat es sie gelöscht. Das kann jedem Anbieter jederzeit passieren. Die Titanic hält die Knute für inakzeptabel und verzichtet auf das Angebot im Playstore. Soviel Unabhängigkeit hat Format. „Je suis Titanic", wenn man so will. Die Witze, um die es geht, sind obszön und respektlos gegenüber der Religion. Man kann sie mit Fug und Recht geschmacklos finden. Als Kunstform darf Satire drastisch, geschmacklos, provokativ und polarisierend sein und einen Finger in die Wunde legen. Als Form des Journalismus greift sie Tagesgeschehen auf und spricht die Themen zuerst im Bauch und dann im Kopf an. Aber hat Google im Play-Store nicht dasselbe Recht, wie jeder Kioskbetreiber, der die Titanic nicht verkaufen will? Nein, weil es an jeder Ecke einen anderen Kiosk gibt, der die Titanic verkauft. Google kontrolliert über den Play-Store 75 % der Smartphone-Inhalte. Der Fall „Titanic" zeigt, dass mit der Wettbewerbsfreiheit zugleich Meinungsfreiheit zerstört wird. Der Gesetzgeber muss den Rahmen der staatlichen Eingriffsbefugnisse gegenüber Unternehmen wie Google erweitern, wenn er ihnen nicht die Hoheit über die Grenzen der Meinungsfreiheit überlassen will.

„Datenschutz-Beauftragter“



Buch + Online-Zugang
Über 50 Muster zum Download

Moos
Datenschutz und Datennutzung
Verträge – Datenschutzklauseln – Datenschutzerklärungen
Herausgegeben von RA, FAITR Dr. Flemming Moos. Bearbeitet von 28 Autorinnen und Autoren. 3. neu bearbeitete und erweiterte Auflage 2021, 1.568 Seiten, Lexikonformat, gbd., mit Datenbankzugang, 139,– €. ISBN 978-3-504-56101-7

Das Werk in weiteren Modulen
otto-schmidt.de/bmds
juris.de/pmds

Mit diesem Formularbuch erhalten Sie das perfekte Werkzeug im Datenschutzrecht: Über 50 praxiserprobte Musterverträge, Klauseln und Datenschutzerklärungen. Es kombiniert detaillierte Einführungstexte und ausführliche Erläuterungen aller Muster Klausel für Klausel. Angepasst an die neueste Rechtsprechung und aktuelle Entwicklungen auf europäischer und nationaler Ebene (z. B. EuGH: Schrems II; Fahion ID; BGH: Cookie-Einwilligung II). Neu in der 3. Auflage: topaktuelle Muster, u.a. zu verbindlichen internen Datenschutzvorschriften für Auftragsverarbeiter, zur Datenschutzerklärung für Beschäftigte/Geschäftskunden und Lieferanten und zur Cookie-Einwilligung sowie Erweiterung des Portfolios englischer Muster.

Nutzen Sie jetzt das gesamte Werk und alle Muster komfortabel online. Inklusive Lawlift-Funktion für ausgewählte Muster.

Gratis-Leseprobe und Bestellung **www.otto-schmidt.de**

ottoschmidt

GDD-FORUM

Ihr Dialog mit der Datenschutz-aufsicht

Erhalten Sie wertvollen Input und stellen Sie Ihre Fachfragen live unseren Experten

10. Mai 2021 | online
Referenten: RA Andreas Jaspers,
Prof. Dr. Rolf Schwartmann, Dr. Stefan Brink,
Barbara Thiel

Jetzt anmelden: **www.datakontext.com**

GDD Gesellschaft für Datenschutz und Datensicherheit e.V.

DATAKONTEXT